DAC beachcroft

Dated: 20th April 2016

Countess of Chester Hospital NHS FT (Data Processor)

- and –

Cheshire Care Record Partner Organisations (Data Controllers)

Cheshire Care Record
Information Sharing and Hosting Agreement

DAC Beachcroft LLP
100 Fetter Lane London EC4A 1BN UK
tel: +44 (0) 20 7242 1011 fax: +44 (0) 20 7831 6630
DX 45 London

Table of contents

Clause heading and number — Page number

1. SCOPE 1
2. INFORMATION TO BE SHARED 2
3. REQUIREMENTS ON ALL PARTIES 2
4. CONSENT AND COMMUNICATION OBLIGATIONS 4
5. ASSURANCE 4
6. KEY CONTACTS 5
7. GOVERNANCE GROUP 5
8. DATA RETENTION 7
9. DE-IDENTIFIED DATA 7
10. AUDIT 8
11. COCH'S SPECIFIC OBLIGATIONS AS HOST 8
12. SUB-CONTRACTING 10
13. LIABILITY AND INDEMNITY 10
14. TERM AND TERMINATION 11
15. CONSEQUENCES OF TERMINATION 11
16. SUBJECT ACCESS AND COMPLAINTS 12
17. FREEDOM OF INFORMATION 12
18. THIRD PARTIES 12
19. NOTICES 12
20. INVALIDITY 12
21. ENTIRE AGREEMENT 13
22. COUNTERPARTS 13
23. LAW AND JURISDICTION 13
24. DEFINITIONS AND INTERPRETATION 13

SCHEDULE 1 – AGREED PARTNER ORGANISATIONS 16

SCHEDULE 2 – DATA ITEMS TO BE SHARED 19

SCHEDULE 3 – USES OF DE-IDENTIFIED DATA 20

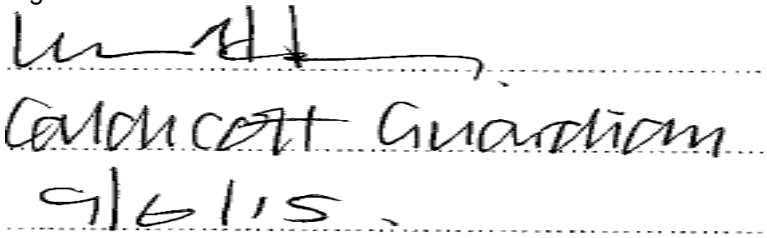
APPENDIX A – FORM OF SCHEDULE 2-16 TO THE SOFTWARE CONTRACT 21

Document Control

Version No.	Author	Date	Amendments	Signature
Final 1.0	Alistair Robertson	June 2015		Signed by all West Cheshire Partners
Final 1.1	Alistair Robertson	June 2015	Wider Cheshire Partners added and contract strengthened re use of de-identifiable data	
Final 1.1	Jackie Millar	July 2015	Reviewed by wider Governance Group	
Final 1.2-1.3	Jackie Millar	Aug 2015	Minor cross referencing amendments	
Final 1.4	Jackie Millar	Nov 2015	Appendix of data items updated	Issued for resigning by all partners to acknowledge extension to the whole of Cheshire and addition of new partners
Final 1.5	Jackie Millar	Mar 2016	1) Appendix of data items updated. 2) Definition of Patient added 3) Section 13.3 strengthened to include financial liability 4) Section 4 – reference to role based access and consenting for differing views removed as these functions have not been utilised in the Cheshire Care Record.	Partners notified of changes
Final 1.6	Jackie Millar	Apr 2016	Schedule 2: Sensitive data exclusions attachment updated	

THIS AGREEMENT is made the 9th day of June 2015

BETWEEN the following parties, each a "**Partner Organisation**", and together the "**Partner Organisations**":

Partner Organisation Name	Countess of Chester Hospital NHS Foundation Trust ("**CoCH**")
Address	Countess of Chester Health Park, Liverpool Road, Chester CH2 1UL
Responsible Manager	Rob Howorth: Deputy Director of Informatics
Contact Details	robert.howorth@nhs.net
Authorised Signatory	Signature: ……  Name: Ian Harvey Position: Medical Director CoCH

Partner Organisation Name	……
Address	……
Responsible Manager	……
Contact Details	……
Authorised Signatory/Date (Caldicott Guardian, SIRO, Chief Executive, Director, GP etc.)	Signature: …… Position: …… Date: ……

This page should be printed, signed, scanned and returned to the Information Governance Manager at the CoCH: Cora.Suckley@nhs.net.

INTRODUCTION:

(A) All the Partner Organisations have agreed to share information about their patients, service users and clients (who for convenience are all referred to in this agreement as "patients") to establish an electronic Cheshire Care Record (**"CCR"**) for the purpose of caring for patients in common.

(B) A list of agreed Partner Organisations is included at Schedule 1. The list can be amended to add or remove Partner Organisations with the agreement of the CCR Information Governance Group.

(C) Each Partner Organisation shall share the agreed Personal Confidential Data extracted from each Partner Organisation's patient records to establish the CCR.

(D) The CCR shall contain Sensitive Personal Data and Personal Data including, but not limited to, medication records, diagnostic results and reports, procedure details, clinical letters, medications, summaries and assessments, appointment/event details, summary social care records and alerts to provide an integrated record for each patient.

(E) Individuals within any Partner Organisation who provide Direct Care for a patient shall be able to access that patient's record electronically at the point of care if appointed access by their Partner Organisation. The CCR shall provide a view only, integrated care record for each individual patient, amalgamated from each Partner Organisation's source systems. This view only functionality shall not allow editing of the source data.

(F) With the explicit approval of the relevant Data Controllers, shared data may be de-identified to Information Standard Board standard 1528 so that it is no longer personal data and can be used for other purposes, subject to agreement by the Governance Group, in accordance with all applicable law and guidance (including, but not limited to, the BMA Confidentiality Toolkit and the Health and Social Care Information Centre Guide to Code of Confidentiality). All uses of de-identified data will be specified within Schedule 3 of this agreement.

(G) The Partner Organisations have agreed to appoint CoCH as the Host of the CCR, and CoCH has agreed to fulfil that role. CoCH shall enter into the Software Contract with the Software Provider, under which the Software Provider shall provide the Software for the CCR. CoCH shall host that Software, and shall provide a first line support service to the Partner Organisations. Second line technical support shall be provided by the Software Provider.

(H) This agreement therefore regulates the sharing of specific Personal Confidential Data between the parties for the delivery of Direct Care to the Partner Organisations' patients. It also regulates the processing of Personal Data by CoCH as the Host on behalf of the Partner Organisations. This is a legally binding agreement.

(I) CoCH has conducted a privacy impact assessment in relation to the CCR proposal, in accordance with the Privacy Impact Assessment Code of Practice published by the Information Commissioner's Office in February 2014.

(J) Each Partner Organisation confirms that its Caldicott Guardian or SIRO has reviewed and agrees with the provisions of this agreement.

NOW IT IS HEREBY AGREED as follows:

1. **SCOPE**

Each Partner Organisation agrees that it is party to this agreement as a data controller in respect of personal data that it discloses, and as a data controller in common in respect of any information that it accesses in the CCR. CoCH in its capacity as Host is a data processor of personal data shared by any of the other Partner Organisations.

2. INFORMATION TO BE SHARED

2.1 Each Partner Organisation shall share the Personal Confidential Data for use in the CCR as defined in Schedule 2.

2.2 The purpose of the information sharing is to create a copy record in the CCR for relevant patients from each Partner Organisation. Partner Organisations providing Direct Care for a patient shall be able to access that patient's CCR record electronically at the point of care. The CCR shall provide a view only integrated care record for each individual patient amalgamated from each Partner Organisation's source systems. This view only functionality shall not allow editing of the data.

2.3 The primary benefit of the sharing is anticipated to be better access for clinicians to a patient's health and social care history at the point of care, leading to better and more well-informed care for that patient.

3. REQUIREMENTS ON ALL PARTIES

General requirements

3.1 Each Partner Organisation shall:

3.1.1 comply with the Data Protection Legislation and all applicable laws;

3.1.2 maintain its registration with the Information Commissioner under the Data Protection Act 1998;

3.1.3 ensure the accurate, timely, secure and confidential sharing of information where such information sharing is essential for the purposes of this agreement;

3.1.4 ensure that information shared pursuant to this agreement is used solely for the purposes set out in this agreement, and is not shared with any other organisation without the prior consent of the relevant Data Controller and/or patient;

3.1.5 respect an individual's right to object to the sharing of Personal Confidential Data about them;

3.1.6 provide staff with training on the principles and legal requirements for information sharing and the appropriate tools to enable them to comply with the obligations under this agreement; and

3.1.7 comply with IGT Requirements 110(116 for GPs), 111 (116 for GPs) and 112(113 for Social Care and 117 for GPs), and make it a condition of employment that all employees, agents or contractors who may access the CCR shall abide by the rules and policies of that Partner Organisation in relation to information governance. This condition shall be written into employment and other contracts and each Partner Organisation shall make staff aware that any failure to comply with the requirements outlined in this agreement is likely to be subject to disciplinary action.

3.2 Each Partner Organisation warrants that the use of information it shares under this agreement in accordance with this agreement shall not cause the user to infringe any third party's intellectual property rights in such information.

Information governance and security

3.3 Subject to clause 3.4, each Partner Organisation shall comply with:

3.3.1 Level 2 of the then current IGT as appropriate to its organisation type and adhere to robust information governance management and accountability arrangements, including effective security event reporting and management; and

3.3.2 the IGT assessment, reporting and audit requirements relevant to its organisation type. Each Partner Organisation shall internally audit its compliance annually and report on such audit to the Governance Group. Each Partner Organisation shall audit CCR access regularly. Each Partner Organisation shall provide other evidence of compliance to the Governance Group or the other Partner Organisations on written request made on behalf of the Governance Group.

3.4 Any Partner Organisation which is a non-NHS organisation and unable to comply with the IGT shall obtain prior written approval from the Governance Group to adopt an alternative, but equivalent standard to the IGT.

3.5 Each Partner Organisation shall have documented policies and procedures to ensure compliance with the national requirements for data protection, information security and confidentiality and be committed to ensuring that any information is shared in accordance with its legal, statutory and common law duties, and, that it meets the requirements of any additional guidance.

3.6 Any Partner Organisation that becomes aware of a Security Incident shall immediately inform the Governance Group and all other affected Partner Organisations with as many details as known at that time. Any affected Partner Organisation (defined as the data controller of the Personal Confidential Data) shall investigate the Security Incident using that Partner Organisation's data loss or data breach procedures. Any affected Partner Organisation shall update the relevant Partner Organisations and Governance Group thereafter, including in respect of the findings of any subsequent investigation report or remedial actions

Access to the CCR

3.7 Each Partner Organisation shall strictly restrict internal organisational access to the CCR for each patient record to those personnel/staff who are providing Direct Care to the relevant patient for that record and who are under written obligations to respect and maintain the confidentiality and security of the Personal Confidential Data and have been properly trained to discharge any relevant obligations in accordance with this agreement.

3.8 This includes access to the CCR by personnel/staff that are providing Direct Care from within the GP Out of Hours Services provided for patients across Cheshire.

3.9 Each Partner Organisation shall use user authentication mechanisms to ensure that all instances of access to the CCR are auditable against an individual, including the following information:

3.9.1 Job role and name of staff member accessing the system;

3.9.2 Organisation name;

3.9.3 What actions were performed; and

3.9.4 The date and time the information was viewed.

4. CONSENT AND COMMUNICATION OBLIGATIONS

4.1 Each Partner Organisation shall:

4.1.1 effectively inform patients about the ways the information they have provided may be used, who it may be shared with, what shall be shared and for what purpose;

4.1.2 effectively inform patients that they have the right to opt out of sharing their information.

4.1.3 effectively inform patients of the implications for the provision of care or treatment, such as the potential risks involved if their full CCR record is not made available to health professionals involved in their Direct Care; and

4.1.4 ensure fair processing notices are always in place.

4.2 Each Partner Organisation shall employ a variety of channels to communicate with its patients regarding information sharing, such as information leaflets, posters, at the point of care, during the patient registration process or when referring into other services.

4.3 Each Partner Organisation shall have a mechanism in place to deal with patients' requests to have their records excluded from the CCR either by excluding such records from their data extracts or by flagging them so that the CCR system does not allow the record to be viewed, until such time as the patient opts back in.

4.4 Patient consent shall be obtained in line with applicable guidance then in force. Provided any disclosure is in accordance with this agreement, each Partner Organisation shall share Personal Confidential Data when it is needed for the safe and effective care of an individual.

4.5 Once a record is held within the CCR, the system prompts for patient consent to be given when a user attempts to access a patient record within the CCR. This is deemed to be good practice, given that the data to be shared includes social and mental health data. The patient can give consent for once only access or for predefined time periods. The system shall then only prompt other users for consent when the consent given expires or for users that are excluded. If patients wish to opt out and remove access to their CCR record after consent has been given they should either request this via their GP or can request that the consent parameters within the CCR system are changed when they next present at any Partner Organisation. A patient may also require any particular Partner Organisation not to share the patient's Personal Confidential Data with the CCR.

4.6 Each Partner Organisation shall ensure that consents it obtains are recorded and a full audit trail retained of who obtained consent.

4.7 If consent is withdrawn, each Partner Organisation shall ensure that withdrawal of consent is recorded and a full audit trail retained of who recorded withdrawal of consent.

5. ASSURANCE

Each Partner Organisation shall:

5.1 take all reasonable steps to ensure the accuracy of the Personal Confidential Data (correct, complete and up-to-date) which it is sharing under this agreement and shall have in place appropriate systems to update any information if subsequently discovered to be inaccurate;

5.2 if it becomes aware of a material inaccuracy or omission in Personal Confidential Data that it shares under this agreement:

5.2.1 inform the recipient of that inaccuracy or omission and take immediate steps to correct or remove the inaccurate information; and

5.2.2 consider whether to inform the data subject, if the data subject is not already aware of the inaccuracy or omission;

5.3 establish a procedure to ensure that only authorised persons access the CCR and ensure that such access is controlled by secure logins and associated audit trails; and

5.4 ensure that Personal Confidential Data for which it is data controller is retained in accordance with its own data retention policy.

6. KEY CONTACTS

6.1 Each Partner Organisation shall nominate a person as a key contact to deal with queries and requests for information under this agreement. For each Partner Organisation that is not a GP practice, this person shall also represent the Partner Organisation in the Governance Group. Such appointed contact shall usually be the Partner Organisation's Caldicott Guardian or SIRO or equivalent.

6.2 A Partner Organisation may change its appointed contact at any time on written notice to the Governance Group.

6.3 The key contact for each Partner Organisation shall ensure dissemination of this agreement in line with each Partner Organisation's internal arrangements for the distribution of policies, procedures and guidelines and monitor the implementation and compliance of this agreement within their own Partner Organisation.

7. GOVERNANCE GROUP

7.1 The purpose of the Governance Group is to collectively exercise control over this agreement and the data processed under it such that the Data Controllers remain Data Controllers in law. This includes overseeing, supporting and maintaining the lawful and secure sharing of information under this agreement.

7.2 The Governance Group shall comprise:

7.2.1 the representative nominated under clause 6.1 by each Partner Organisation that is not a GP practice.

7.2.2 one individual chosen by all the Partnership Organisations that are GP practices for each GP locality to represent those Partnership Organisations;

7.2.3 a patient representative of each GP locality, which the parties agree may be nominated by any of the Partner Organisations and appointed by the Governance Group.

7.3 Each Partnership Organisation (or group of GP practice Partnership Organisations representing a locality as the case may be) shall determine how to nominate its representative and the term and other conditions of that nomination.

7.4 The Governance Group shall meet at least every three months or at such other interval as the Governance Group shall determine.

7.5 The Governance Group shall have the following powers and responsibilities:

7.5.1 debate all proposed changes to the purpose and processing of data and submit these to all Data Controllers for consideration in accordance with clauses 7.8 and 7.9 of this agreement;

7.5.2 to approve additional Partner Organisations joining this agreement;

7.5.3 to determine whether a Partner Organisation shall cease to be a party to this agreement for a specific period of time or permanently for non-compliance;

7.5.4 to determine whether a Partner Organisation may derogate from or amend any requirement under this agreement;

7.5.5 to maintain an information conduit between the Partner Organisations;

7.5.6 to investigate breaches of the agreement and require Partner Organisations to take remedial actions;

7.5.7 to monitor each Partner Organisation's compliance with this agreement. The Governance Group may request evidence of compliance with this agreement on written request to any Partner Organisation;

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

7.5.9 to approve common patient communication materials; and

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

7.6 The Governance Group shall appoint a Chair, and one or more individuals to receive and distribute communications on its behalf.

7.7 The Governance Group may regulate its own procedures (including by agreeing conditions of appointment and removal for patient representatives) subject to the provisions of this agreement.

7.8 The Governance Group may approve the following things provided that the requirements of clause 7.9 are met:

7.8.1 the use of data for other purposes related to the purposes of this agreement;

7.8.2 amendments to this agreement;

7.8.3 the appointment of any new Sub-contractor.

7.9 The Governance Group may approve any of the things listed in clause 7.8 provided that:

7.9.1 it is satisfied that it is lawful to do so;

7.9.2 all Partner Organisations have been 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 (and any Partner Organisation that does not wish to participate has been given the opportunity not to do so); and

7.9.3 any additional purpose for using the data is related to the purpose of this agreement.

7.10 The Governance Group may only approve the de-identification of data with the explicit approval of all affected data controllers.

7.11 Governance Group decisions shall be taken by consensus. Before any Governance Group decision is taken, members shall satisfy themselves that they are authorised to do so (i.e. where relevant, at IG lead / Caldicott Guardian /SIRO level) by those they represent.

7.12 If consensus on any decision cannot be reached, and unless the Governance Group decides otherwise, its decisions shall be taken by a simple majority, or where there is no majority the Chair of the group has a casting vote.

8. DATA RETENTION

8.1 An initial data upload is extracted and processed for inclusion in the CCR. This is retained as a "delta" feed. Changes to that data are replaced through real time or subsequent data feeds. If a patient chooses to opt out, the GP Partner Organisation can flag their record for exclusion and the data is purged from the system. If the patient opts back in then a new bulk upload for that patient occurs and adds any data from the date that the patient was removed back into the delta feed. This provides flexibility to quickly reinstate the record if the patient should change their mind and opt back in. Alternatively the Partner Organisation can exclude the patient's data from their extract. If a data controller ceases to participate in the CCR that data controller's data is removed at the next extract.

8.2 Data that is stored and generated within the CCR, including audit trails, access logs, etc, are retained in accordance with General Medical Council and British Medical Association guidance and the NHS Records Management Code of Practice.

8.3 The 'delta' feed will be reviewed annually by the Clinical Design Authority to ensure that the content of the CCR is appropriate for its intended use. Data that is no longer deemed to be relevant will be cleansed from the CCR.

8.4 The audit log will be retained for ten years.

9. DE-IDENTIFIED DATA

9.1 If any De-identified Data is produced in accordance with introductory clause **Error! Reference source not found.**, Partner Organisations may access that De-identified Data provided that no Partner Organisation shall:

9.1.1 Attempt to re-identify any De-identified Data;

9.1.2 Use any De-identified Data to identify any individual;

9.1.3 Use any De-identified Data to take a decision about any specified individual or individuals;

9.1.4 Share data contained within the De-identified Data with any third party, apart from a third party engaged by a Partner Organisation to act on behalf

of that Partner Organisation, for the sole purpose of that third party acting on behalf of that Partner Organisation, and where that third party is subject to contractual terms no less onerous than those imposed on Partner Organisations by this agreement;

9.1.5 Link any De-identified Data with any other dataset containing personal data; or

9.1.6 Sell or otherwise exploit for commercial gain or reward any De-identified Data.

9.2 A Partner Organisation (other than a local authority) may only use or allow any De-identified Data to be used in connection with that Partner Organisation's statutory functions as a provider of health and/or social care.

9.3 A Partner Organisation which is a local authority may only use or allow any De-identified Data to be used in connection with that Partner Organisation's statutory functions as a provider or commissioner of health and/or social care.

9.4 The Governing Group may authorise any CCG to use De-identified Data, provided that the CCG complies with this clause 9 and only uses or allows any De-identified Data to be used in connection with its statutory functions as a commissioner of health care.

10. AUDIT

10.1 Each Partner Organisation accepts responsibility for independently or jointly auditing its own compliance with this agreement at least annually.

10.2 The Governance Board may commission, at its discretion to be supported by all parties:

10.2.1 audits of COCH compliance with this agreement

10.2.2 audits of the software provider or any approved sub processor compliance with this agreement

11. COCH'S SPECIFIC OBLIGATIONS AS HOST

In its capacity as Host, CoCH shall:

11.1 Enter into the Software Contract. CoCH shall manage and enforce the provisions of the Software Contract against the Software Provider.

11.2 Host the software required to use the CCR in accordance with the Warranted Environment Specification (WES) stated within the Software Contract.

11.3 Provide a first line technical support service for the CCR, and contract with the Software Provider for the Software Provider to provide a second line technical support service.

11.4 Work with the Software Provider to provide:

11.4.1 implementation and set-up assistance for the CCR; and

11.4.2 training for each Partner Organisations Trainers to enable cascade training to end users of the CCR.

11.5 Comply with its obligations as a data processor, and specifically shall (and shall ensure that the Software Provider shall):

11.5.1 process the personal data only in accordance with instructions from the Governance Group, which may be specific instructions or instructions of a general nature as set out in this agreement or as otherwise notified by the Governance Group to CoCH during the term of this agreement;

11.5.2 process the personal data only to the extent, and in such manner, has been approved by the Governance Group, as is necessary for the purposes of this agreement or as is required by law or any regulatory body;

11.5.3 take reasonable steps to ensure the reliability of any CoCH or Software Provider (as the case may be) personnel who have access to the personal data;

11.5.4 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;

11.5.5 obtain prior written consent from the Governance Group before transferring any personal data to any sub-contractors;

11.5.6 ensure that all CoCH or Software Provider (as the case may be) personnel required to access the personal data are informed of the confidential nature of the personal data and comply with the obligations set out in this clause 11;

11.5.7 ensure that none of the CoCH or Software Provider (as the case may be) personnel publish, disclose or divulge any of the personal data to any third party unless directed in writing to do so by the Governance Body;

11.5.8 notify the Governance Group within five working days if it receives:

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

(b) a complaint or request relating to CoCH's obligations as Host under the Data Protection Legislation;

11.5.9 provide the Governance Group and any Partnership Organisation with full cooperation and assistance in relation to any complaint or request made, including by:

(a) providing full details of the complaint or request;

(b) complying with a data access request within the relevant timescales set out in the Data Protection Legislation and in accordance with the Governance Group or relevant Partner Organisation's reasonable instructions;

(c) providing the Governance Group or relevant Partner Organisation with any personal data it holds in relation to a data subject (within the timescales reasonably required by the Governance Group or relevant Partner Organisation); and

(d) providing the Governance Group or relevant Partner Organisation with any information reasonably requested by the Governance Group or relevant Partner Organisation;

11.5.10 permit the Governance Group (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit CoCH's data processing activities and comply with all reasonable requests or directions by the Governance Group to enable the Governance Group to verify and/or procure that CoCH in its capacity as Host is in full compliance with its obligations as Host under this agreement;

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

11.5.12 not transfer any personal data outside the European Economic Area.

11.6 Not make any further copies of the personal data, except for back-up copies as necessary, and except where de-identified in accordance with this agreement or approved by all Partner Organisations.

11.7 Carry out its obligations under this agreement in compliance with Data Protection Legislation.

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

11.9 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.

11.10 Maintain and implement a business continuity and disaster recovery plan to the reasonable satisfaction of the Governance Group.

11.11 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 Governance Group. These should occur at least once in every three years.

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

11.13 Ensure that on the expiry or termination of this agreement, the Personal Confidential Data is returned to each Partner Organisation, destroyed, or migrated to an alternative software provider and shall ensure that no Personal Confidential Data is retained by the Software Provider.

12. SUB-CONTRACTING

12.1 The Governance Group may from time to time authorise CoCH to authorise a third party ("**Sub-contractor**") to process Personal Confidential Data on behalf of the Partner Organisations. At the date hereof, CoCH is hereby authorised to appoint the Software Provider as a Sub-contractor.

13. LIABILITY AND INDEMNITY

13.1 Each Partner Organisation shall accept responsibility, including financial responsibility, for its own acts and omissions and those of its employees and contractors acting under their direction and control.

13.2 CoCH's liability, in its capacity as Host, shall be limited to £500,000.

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

13.4 Each Partner Organisation warrants that in accessing the CCR it shall comply with the licence terms set out in Schedule 2-16 to 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 legal and other professional costs and expenses) arising out of or in connection with:

13.4.1 the use of shared data by the Partner Organisation;

13.4.2 personal injury caused by or arising from the Partner Organisation's use of shared data;

13.4.3 the Partner Organisation's failure to comply with the licence terms in Schedule 2-16 of the Software Contract; or

13.4.4 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.

14. TERM AND TERMINATION

14.1 This agreement shall commence on the Commencement Date and shall, unless extended or terminated, expire on the fourth anniversary of the Commencement Date.

14.2 If CoCH extends the Software Contract with the prior approval of the Governance Group, the term of this agreement shall automatically extend in line with that of the Software Contract. This clause shall not affect any party's rights under or limit the application of 14.3 to 14.5.

14.3 A Partner Organisation, which is considering terminating its participation in this agreement shall notify the Governance Group of its intention and reasons, and agrees to liaise with the Governance Group for at least four weeks, before giving notice of termination, to ascertain whether its concerns can be addressed. Having done so, a Partner Organisation may terminate its participation in this agreement by giving three (3) months' written notice.

14.4 The Governance Group may decide to terminate this agreement.

14.5 This agreement shall immediately terminate in the event of the termination for whatsoever cause of the Software Contract.

15. CONSEQUENCES OF TERMINATION

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

15.1.1 the exiting Partner Organisation shall cease accessing the CCR immediately and securely return or destroy any shared information in its possession;

15.1.2 CoCH as Host shall arrange for the cessation of the exiting Partner Organisation's access to the Software; and

15.1.3 CoCH as Host shall ensure that Personal Confidential Data for which the exiting Partner Organisation is data controller is removed from the CCR at the next extract following the Partner Organisation's exit.

15.2 Any former Partner Organisation shall have access to audit trails only on the written authority of the Governance Group or as required by law.

16. SUBJECT ACCESS AND COMPLAINTS

16.1 Each Partner Organisation is responsible for putting into place effective procedures to address complaints about data sharing and subject access requests relating directly to this agreement. Information about these procedures should be made available to patients.

16.2 Each Partner Organisation shall have a designated Data Protection Officer, Information Governance Manager or other nominated manager who is responsible for subject access requests and complaints.

16.3 Subject access requests from third parties for data available to organisations under this agreement are to be directed promptly to the Data Protection Officer, Information Governance Manager or relevant nominated manager for dealing with subject access requests of the relevant Partner Organisation.

16.4 Any complaints about data sharing relating directly to this agreement should be directed promptly to the Data Protection Officer or Information Governance Manager of the relevant Partner Organisation and dealt with in accordance with the policy of that Partner Organisation.

17. FREEDOM OF INFORMATION

The Partner Organisations recognise that public bodies are subject to the requirements of the Freedom of Information Act 2000 ("**FOIA**") and the Environmental Information Regulations 2004 ("**EIR**"). Any such requests relating to information governed by this agreement should be directed promptly to the Data Protection Officer or Information Governance Manager of the relevant Data Controller.

18. THIRD PARTIES

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

19. NOTICES

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

20. INVALIDITY

In the event that any provision of this agreement 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 agreement, which shall continue to be valid to the fullest extent permitted by law.

21. **ENTIRE AGREEMENT**

This agreement constitutes the entire agreement relating to its subject matter and supersedes all previous verbal or written proposals and agreements between the Partner Organisations.

22. **COUNTERPARTS**

22.1 This agreement 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.

22.2 The agreement shall not be effective until CoCH and at least one other signatory has executed a counterpart.

22.3 Any Partner Organisation, which executes a counterpart after the Commencement Date shall be bound by the terms of this agreement from the date of that Partner Organisation's signature.

23. **LAW AND JURISDICTION**

This agreement shall be governed by and construed in all respects in accordance with the laws of England and each Partner Organisation hereby submits to the exclusive jurisdiction of the courts of England.

24. **DEFINITIONS AND INTERPRETATION**

24.1 In this agreement the following terms shall have the meanings given to them in the Data Protection Act 1998: **"data controller", "data controller in common", "data processor", "data subject", "personal data", "process", "processing", "processed", "sensitive personal data"**.

24.2 In this agreement unless the context otherwise requires the following words and expressions shall have the following meanings:

"Auditors"	means the data controller, its auditors, advisors, any regulatory body or other agents;
"Commencement Date"	means the date of commencement of live operation of Carecentric with real patient data;
"De-identified Data"	means any data that has been de-identified in accordance with introductory clause (F);
"Direct Care"	means a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care;

"Data Protection Legislation"	means the Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 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;
"Governance Group"	means the group defined in clause 7;
"GP locality"	means an area covered by a CCG;
"IGT"	means the NHS Information Governance Toolkit, as may be amended and updated from time to time;
"patient"	means the generic term used within this agreement to refer to a person who is eligible for or who has a summary Cheshire Care Record and is being treated by one of the partner organisations, otherwise referred to as clients, residents, service users, citizens or people.
"Personal Confidential Data"	means personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this agreement '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 sensitive personal data;
"Security Incident"	means an actual, suspected or threatened unauthorised exposure, access, disclosure, use, communication, deletion, revision, encryption, reproduction or transmission of any component of Personal Data or unauthorised access or attempted access to any Personal Data within the Cheshire Care Record;
"Software Contract"	means the contract dated on or about the date of this agreement between CoCH and the Software Provider for the provision of the software required to use the CCR;
"Software Provider"	means Softcat Limited, a company registered in England and Wales (registered number 2174990) whose registered office is at Morton House, Thames Valley Industrial Park, Marlow, Bucks SL7 1TB, and includes Softcat Limited's subcontractors, including Graphnet Health Ltd (Company registered in England No. 02933905) whose registered office is at Station House, Station Road, Newport Pagnell MK16 0AG.

24.3 Unless the context otherwise requires, the singular includes the plural and vice versa.

24.4 The headings in this agreement are for the convenience of the Partner Organisations only, and are in no way intended to affect, describe, interpret, define or limit the scope, extent, or interpretation of the agreement of any provision thereof.

24.5 Any obligation in this agreement not to do anything includes an obligation not to suffer, permit or cause that thing to be done.

24.6 The terms "**including**", "**includes**", and "**in particular**" shall not be construed as terms of limitation.

24.7 Reference in this agreement to any directive, regulation, decision, statute, enactment, or other similar instrument shall be construed to include a reference to such instrument, as the same is from time to time amended, extended, re-enacted, replaced, or consolidated.

SCHEDULE 1

AGREED PARTNER ORGANISATIONS

- 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)
- Countess of Chester NHS FT (CoCH)
- Clatterbridge Cancer Centre NHS Trust.

GP Practices South Cheshire CCG

Area	**Practice**
Alsager	Cedars
Alsager	Merepark
Alsager	Rode Heath
Alsager	Scholar Green
Crewe	Delamere Street
Crewe	Earnswood
Crewe	Gresty Brook
Crewe	Grosvenor
Crewe	Haslington
Crewe	Hungerford
Crewe	Millcroft
Crewe	Rope Green
Middlewich	Watersedge MC
Middlewich	The Oaklands
Nantwich	Nantwich Health Centre
Nantwich	Kiltearn
Nantwich	Tudors
Sandbach	Ashfields PCC
Audlem	Audlem
Wrenbury	Wrenbury Surgery

GP Practices Vale Royal CCG

AREA	**PRACTICE**
Northwich	Danebridge
Northwich	Firdale Medcal Centre
Northwich	Kingsmead
Northwich	Middlewich Road
Northwich	Oakwood MC
Northwich	Sandiway
Northwich	Watling Street
Northwich	Weaverham

Northwich	Witton Street
Winsford	High Street
Winsford	Launceston
Winsford	Swanlow Lane
Winsford	Weavervale
Winsford	Willow Wood

GP Practices Eastern Cheshire CCG

Area	**Practice**
Knutsford	Annandale Medical Centre
Macclesfield	Bollington Medical Centre
Macclesfield	Broken Cross Surgery
Chelford	Chelford Surgery
Macclesfield	Cumberland House
Alderley Edge	George Street Surgery
Handforth	Handforth Health Centre
Macclesfield	High Street Surgery
Holmes Chapel	Holmes Chapel Health Centre
Wilmslow	Kenmore Medical Centre
Congleton	Lawton House Surgery
Knutsford	Manchester Road Medical Centre
Macclesfield	McIlviride Medical Practice
Congleton	Meadowside Medical Centre
Macclesfield	Park Green Surgery
Macclesfield	Park Lane House Medical Centre
Poynton	Priorsleigh Medical Centre
Congleton	Readesmoor Medical Group Practice
Macclesfield	South Park Surgery
Stockport	The Schoolhouse Surgery
Knutsford	Toft Road Surgery
Macclesfield	Vernova Healthcare Cic
Wilmslow	Wilmslow Health Centre

GP Practices West Cheshire CCG

Boughton Health Centre
City Walls Medical Centre
Elms Medical Centre
Farndon
Frodsham Medical Practice
Great Sutton - Dr Faulks
Great Sutton - Dr McAlvery
Great Sutton - Dr Wearne

Handbridge
Heath Lane
Helsby Health Centre
Kelsall Medical Centre
Knoll Surgery
Lache Health Centre
Malpas Medical Centre
Neston Medical Centre
Neston Surgery
Northgate Village
Old Hall Surgery
St Werburghs
Tarporley - Dr O'Callaghan
The Rookery
Upton Village Surgery
Western Avenue
Westminster Surgery
Whitby GP - Dr Burgess
Whitby GP - Dr Stringer
Whitby GP - Dr Warren
Willaston Surgery
York Road
Garden Lane
Hoole Surgery
Park Medical Centre
Bunbury
Northgate St MC
Tarporley - Dr Gleek

SCHEDULE 2

DATA ITEMS TO BE SHARED – Updated Mar 2016 to Final version 1.0

Cheshire Care Record data items v1.0.xl

Sensitive Data exclusions

Cheshire Care Record Sensitive Data Exc

SCHEDULE 3[1]

Uses of De-Identified Data

Partner Organisation (Data Controller)	Data items to be de-identified	Purpose	Signature to authorise use

[1] There are no plans to de-identify any extracted data as of May 2015, but this schedule has been designed to accommodate this in the future if required

[2] Contract amendments have been made to add each new Partner Organisation to the Graphnet contract as

APPENDIX A

FORM OF SCHEDULE 2-16 TO THE SOFTWARE CONTRACT

SCHEDULE 2-16

SOFTWARE AND SOFTWARE LICENCE TERMS

1. INTRODUCTION

1.1. This Schedule details the various elements of the Software and categorises them into CONTRACTOR Software and Third Party Software.

1.2. Annexes A and B of this Schedule sets out the licence terms for the CONTRACTOR Software and Third Party Software (including Open Source Ordered Software), respectively.

1.3. The CONTRACTOR shall update this Schedule periodically to record any software subsequently acquired from third parties or developed for the delivery of the Ordered IT Products.

2. CONTRACTOR SOFTWARE

2.1. The CONTRACTOR Software comprises the following items: Not used

3. THIRD PARTY SOFTWARE

3.1. The Third Party Software shall consist of the following items, including any Open Source Ordered Software:

Software	Supplier	Purpose	[Number of Licences]	[Restrictions]	Number of Copies]	[Other]
CareCentric Gateway (including CareCentric embedded)	Graphnet Health Ltd			As set out in Annex B	1	
Care Centric Highway Instance	Ditto			ditto	1	
	Ditto			ditto	1	
Care Centric Mobile	Graphnet Health Ltd under licence from Shearwater Systems Ltd		100 End User Device licences for the CUSTOMER	ditto	1	

Annex A to Schedule 2-16 of the Software Contract

CONTRACTOR Software

Not used

Annex B to Schedule 2-16 of the Software Contract

Third Party Software

In these licence terms (and where the context so requires in this Contract) the following words and phrases will the meanings assigned to them as follows:

"End User"	means employees, contracted staff, principles or partners of the CUSTOMER and or of the Service Recipient Organisations permitted by the CUSTOMER to use the Third Party Software.
"Service Recipient Organisations"[2]	Means the following organisations: Cheshire West and Cheshire Council Cheshire & Wirral Partnership NHS Foundation Trust Clatterbridge Cancer Centre NHS Foundation Trust The following: General Medical Practices: Implemented at up to 37 GP practices of which Graphnet has been given prior written notice (including notification of the practice's name and address). As all these recipient organisations are structured and operated at the date of this Contract. Additional Service Recipient Organisations may be added under the Change Control Procedure. The substitution of one GP practice for another will be regarded as the implementation at a new GP practice Service Recipient Organisation but

[2] Contract amendments have been made to add each new Partner Organisation to the Graphnet contract as new service recipients, in accordance with the Partner Organisation list in Schedule 1.

	will only be the subject of additional Charges if and to the extent that the substitution would take the number of GP implementations beyond the 37 on which the Charges are based)
"Supplier"	means the proprietary owners of the software listed in column 2 in the table in paragraph 3.1 of this schedule 2-16 to this Contract.

1. The suppliers of the software as listed in column 2 of the table in paragraph 3.1 in this schedule 2-16 licence their [Third Party] Software on the following general and specific terms and conditions:

   1.1. General terms and conditions applicable to all the Third Party Software:

      1.1.1. The Suppliers grant to the CUSTOMER and the Service Recipient Organisations (and the CUSTOMER and the Service Recipient Organisations accept) a non-exclusive, non-transferable licence for the registered End Users of the CUSTOMER and each Service Recipient Organisations to use the [Third Party] Software (other than the CareCentric Mobile software product) for the treatment and or care of their patients within the geographical areas covered by the normal operations of the CUSTOMER and each Service Recipient Organisations as at the date of this Contract and in their respective testing and training environments. The licence for the use of the Care Centric mobile software is granted to the CUSTOMER only for the use of its authorised end users for the treatment and care of its patients and in its respective testing and training environments only).

      1.1.2. The licences granted in paragraph 1.1.1 are subject to the following conditions:

         1.1.2.1. There shall be no sub-licencing to any third parties.

         1.1.2.2. The licences subsist only during the period that the Suppliers are contracted directly or indirectly to support and maintain the [Third Party

Software] and for which the required charges and licence fees have been paid.

1.1.2.3. The CUSTOMER and the Service Recipient Organisations shall not (and shall procure that their End Users shall not):

1.1.2.3.1. copy reverse engineer, de-compile, or disassemble the licenced software except to the extent the Suppliers cannot prohibit by law;

1.1.2.3.2. remove any trademark, trade name or copyright notice or other notice from the software.

1.1.2.4. The CUSTOMER shall indemnify and keep indemnified the Suppliers 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 legal and other professional costs and expenses) arising out of or in connection with:

1.1.2.4.1. personal injury caused by or arising from the use of CUSTOMER Data (except such caused by the negligence of a Supplier); or

1.1.2.4.2. the infringement of the rights of any third party arising out of the possession, processing or use of CUSTOMER Data (except where such failure or infringement is as a result of the negligence of the Supplier or their breach of their obligations under the terms of the agreement under which the Ordered IT Products are supplied).