

## **Child Health Information Service**

### **Sign-up Document for Data Supply, Sharing & Access Agreement**

**Between Bristol City Council for**

**a) School Enrolment Provider (relating to School-  
Aged Immunisations),**

**and**

**b) Looked After Children Provider**

**c) Public Health Access**

**and**

**the South West Child Health Information Service**

**Date: 11th July 2018**

**Version: 6.0**



## GUIDANCE NOTE

### Introduction

This guidance note is intended to provide your organisation with an explanation on the status and remit of the Child Health Information Service (CHIS) for the South West (the “**Service**”). The Secretary of State delegates a number of his/her public health functions to NHS England. The public health functions agreement 2017 – 2018 enables NHS England to commission certain public health services which will drive improvements in population health, and this agreement sets out the service specifications which are to be commissioned in order to satisfy those public health functions. One such service is the CHIS, and so it is commissioned by NHS England in order to discharge part of their public health duties. The CHIS initiative therefore follows a tender process by NHS England South (South West) which resulted in the appointment of Health Intelligence Ltd (HI) on a 5-year contract to deliver the South West CHIS commencing in stages between 1<sup>st</sup> April 2018 and 1<sup>st</sup> July 2018. A single South West (SW) CHIS database will replace the 5 incumbent CHIS provider databases.

Commencing on the 1<sup>st</sup> April 2018 in most of Devon and from the 1<sup>st</sup> July 2018 for Cornwall & Isles of Scilly and Bristol, North Somerset, Somerset and South Gloucestershire (BNSSSG), the CHIS will facilitate the collation, analysis and reporting on child health services for the South West. The CHIS will facilitate the appropriate access by authorised organisations to the child health record. A single South West CHIS service will replace the five incumbent CHIS provider services.

The overarching Data Sharing Framework should be reviewed prior to this Data Sharing Agreement and both will need to be signed prior to data sharing. This Agreement (the “**Agreement**”) confirms the data to be shared by your organisation with the Service and which organisations will access this data. It also confirms your Organisation’s access to the child health records stored within the South West CHIS. Another component of the agreement is a “**Data Processing Contract**” between your organisation as the Data Controller and the CHIS Provider as the Data Processor.

All organisations providing Personal Data to the Service will be “**Data Controllers**”. Health Intelligence will ensure that the level of access agreed within this document and similar agreements are reflected within the information systems and interfaces established to facilitate appropriate sharing of child health records. To assist them and other Data Controllers, an IG Sub Group of the South West CHIS Service Board will be formed from the provider organisations who will share information with the Service; they will approve access to the Service noting restrictions (e.g. to the scope of the data that may be accessed) for those child health records that are appropriate to the organisation concerned.

Your organisation along with other organisations providing Personal Data to the CHIS will be able to access your children’s records in support of direct patient care. Once in agreed form this Agreement will support the Service to meet its strategic objectives namely to “Know where every child is” and “How well they are” through the modernisation of Child Health Information Systems and their new focus on collecting, collating, analysing and reporting.

Supported by this Agreement, the organisations that may access the child health records (at various levels) are detailed in SCHEDULE 2 of the Agreement.

The CHIS Provider (Health Intelligence Ltd) will be the Data Processor acting on the directions of the Data Controllers.

### Governance

NHS England South (South West) has reviewed these proposed arrangements to confirm their appropriateness. It is, however, for each organisation to confirm they agree to participate in this initiative by entering into the Agreement. As a Data Controller (alongside other providers of child health services – and referenced as Data Controllers), the organisation confirms in line with SCHEDULE 2 the organisations that may access the Personal Data provided by your organisation to the Service.

Similarly, this Agreement supports your Organisation in line with SCHEDULE 3, within the stated limits, to access the data hosted for your children provided by other Data Controllers. Health Intelligence,



will be the Data Processor, and will take a lead role in facilitating the provision of access. Health Intelligence will only process/share Personal Data as detailed within this Agreement and similar Agreements. These controls are designed to facilitate the legitimate sharing of child health data (including maternal data) it receives from General Practice and others health and social care organisations.

### **Legal Basis for Sharing**

#### The legal basis

The processing and sharing of data with the other NHS and Social Care Organisations is for medical purposes and is being initiated by your Organisation – the “**Participant**”. Health Intelligence will take receipt of relevant patient data on behalf of the Participant; and host and process data as reflected by its contract with NHS England South (South West) and the restrictions set out in this document and similar documents with the other Data Controllers contributing to the CHIS. Health Intelligence will ensure it only processes data as reflected by this and similar Agreements, and in accordance with the Data Protection Act 1998 ("DPA") until 25 May 2018, and thereafter the General Data Protection Regulation ("GDPR")/Data Protection Bill (as enacted).

Under both the current and impending new data protection regime, personal data must be processed lawfully, fairly, and transparently. There must be a lawful basis for processing, as set out either under the DPA or GDPR (once effective) by satisfying one of the conditions in Schedule 2 of the DPA/Article 6 of GDPR. In addition, as this involves data relating to a patient's health then it is sensitive personal data (or, as it will be known under GDPR, special categories of personal data).

The processing (either by sharing the data with the CHIS, or by accessing it) is necessary for the pursuit of legitimate interests by the Data Controllers which satisfies Condition 6(1) of Schedule 2, DPA. However, under GDPR Data Controllers who are public bodies cannot rely upon the legitimate interest basis for processing unless they are acting outside of their functions as a public authority. They can, however, rely upon Article 6(1)(e) instead which applies to tasks carried out in the public interest.

Moving onto the additional basis for processing required by sensitive/special categories of personal data, provision of care and treatment (8th condition of SCHEDULE 3 of the DPA) and Article 9(2)(h) of GDPR apply similarly in that personal data can be processed where it is necessary to do so for medical purposes by a healthcare professional, albeit GDPR has been expanded somewhat to also include Social Care Activities. The sharing of patient identifiable data (PID) will only take place with the Data Controllers who participate in the CHIS, however other organisations are able to access patient level, but Anonymised Data and Aggregate Only data (as detailed in SCHEDULE 2). In addition, The Childcare Act 2006 details the statutory responsibilities of Local Authorities when planning and providing services for families with young children.

Under GDPR, Data Controllers will be expected to be much more transparent with patients about how their data will be processed. For the reasons outlined above, you will not need patient consent to share and access information through the CHIS. However, your Fair Processing Notices/Privacy Notices should explain that data will be shared with the CHIS.

In addition to the requirements of the data protection legislation, any sharing of personal data must also take place in accordance with the common law duty of confidentiality. The duty does not require consent from a patient where the proposed use of their data is in the public interest (which it is here) as it directly benefits patient and public health. Good practice suggests that although consent is not required, patients should be told how their data will be used and this should be set out in your Fair Processing Notice (as referenced in the previous paragraph). This is a matter for all Data Controllers to address themselves.

The flow of patient identifiable data concerning children aged 0-18 inclusive between the Participant and the local CHIS occurs presently and is an established information flow although there is a new provider of the SW CHIS and a rationalisation of the numbers of providers and systems; rather than 5 incumbent CHIS providers each with their own CHIS, from April 2018 there will be a single SW CHIS. To support service continuity, there will be four local CHIS Offices, Truro, Plymouth, Exeter and

Bridgwater.

These existing flows of patient data are recognised matters of public health.

The flow of patient data includes administrative data to ensure a record for all GP Practice registered children and resident children is maintained on the CHIS database. Relevant clinical data is also provided to support the Healthy Child Programme.

These flows of patient data from the Participant to the CHIS have a legal basis and is “business as usual”. Currently some of the information flows occur on paper, the only difference reflected in this Agreement is that the scope of the data to be exported is being formalised and the data exports will be undertaken electronically.

Some aggregate only data (numbers and percentages only) will be shared with NHS England and coterminous Local Authorities. Whilst the DPA 1998/GDPR and Health & Social Care Act 2006 are concerned with the appropriateness of sharing patient identifiable data, anonymised or aggregate data are not subject to these Acts, provided that the patients cannot be identified from the data.

#### **How the data will be shared**

There are a range of solutions to be delivered by the Service, over time paper-based and e-mail based methods will be replaced with CSV file based data sharing arrangements which in term will be replaced by modern and secure messaging e.g. HL7 and FHIR. Investments are being made to modernise the information flows in support of this data sharing.

#### **Security Arrangements**

A key issue for all concerned is ensuring the security of personal data. The Agreement (along with this Guidance Note) has been reviewed by NHS England South (South West).

Security within the solution is multi-layered and extremely rigorous, helping to ensure that patient confidentiality is preserved at all times. The CHIS system, under formally contractual arrangements, will be provided by System C Healthcare Ltd and is known as CarePlus; it is browser based and makes use of NHS smart card access controls. The HI Hub system provided by Health Intelligence will support data from General Practice to be exported and loaded and facilitate enhanced reporting for the CHIS. Both CarePlus and HI Hub will only be accessible over N3/HSCN.

Health Intelligence is ISO27001:2013 Security Management System certified and undergoes regular internal and external audits to ensure full compliance with data security regulations. All parties to this Agreement affirm their compliance to the Department of Health’s Information Security Management: NHS Code of Practice (2007).

The obligations imposed under this Agreement also apply to any agreed extensions to the scope of data to be hosted.

#### **Information Governance Arrangements**

Another key issue is that of Information Governance in general and specifically compliance with the various Acts and NHS best practice associated with sharing and processing personal data. In support of the requirement to inform patients regarding the arrangements for hosting and processing their data, we will provide a poster for display on patient notice boards. Strengthened by GDPR requirements, it is the Participant’s responsibility to be transparent about how personal data is being used and who it is being shared with. The Poster assists with meeting the Fair Processing Notice/Privacy Notice obligations and can be complemented by additional material hosted on the organisation’s web sites in support of compliance with the DPA/GDPR. We recommend that your Fair Processing Notices reflect the information sharing and processing which will take place under the Agreement.

#### **Confidentiality Arrangements**

The Agreement confirms who may access patient data, for what purpose access is required and which specific level of access will be granted (for example, Aggregate Only (numbers and percentages), Patient Level but Anonymised or Patient Identifiable Data (“PID”)).



Only the parties identified in SCHEDULE 2 of the Agreement shall have access to the patient's data exported from your organisation.

**Security Incidents:**

Any actual or perceived security incidents will be handled in line with the provisions of the Agreement and in line with the Department of Health's Information Security Management: NHS Code of Practice (2007).

**Who to contact for more information:**

If you have any specific questions around the Agreement, please feel free to contact the HI's Support Desk on: (01270) 527 373.

**Who to contact for more information:**

If you have any specific questions around the Agreement, please feel free to contact the HI's Support Desk on: (01270) 527 373.

**For further information please contact:**

Mr Michael Pennington,  
Data Protection Officer  
Health Intelligence Ltd  
Saxon House  
Moston Road  
Sandbach  
Cheshire  
CW11 3HL  
Email: [dpo@health-intelligence.com](mailto:dpo@health-intelligence.com)  
Tel: 01270 765124

Alternatively, please email HI on: [supportdesk@health-intelligence.com](mailto:supportdesk@health-intelligence.com)




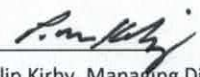
**Please send your signed agreement to:**

Ms Stephannie Cargill,  
Support Services Team,  
Health Intelligence Ltd,  
Saxon House,  
Moston Road,  
Sandbach,  
Cheshire,  
CW11 3HL



## DATA SUPPLY, SHARING AND ACCESS AGREEMENT

<b>CONTRACT SHEET</b>	
<b>PARTIES</b>	
<ul style="list-style-type: none"> <li>Health Intelligence Ltd ("HI") a company incorporated in England with company number 03257228 whose registered office is at Beechwood Hall, Kingsmead Road, High Wycombe, England, HP11 1JL ("CHIS Provider") and</li> <li>Bristol City Council operating from City Hall, PO Box 3176, Bristol BS3 9FS (the "Participant"), (each a "party" and together the "parties").</li> </ul>	
<b>BACKGROUND</b>	
<ul style="list-style-type: none"> <li>HI has been commissioned to provide the South West Child Health Information Service (CHIS) (the "Service") by NHS England South (South West) from the 1<sup>st</sup> April 2018 for a term of 5 years. Personal data will be collected, collated, analysed and reported on and made available to other organisations involved in the commissioning, service provision and safeguarding of children; they will access data at an appropriate level making use of CarePlus (the "System C Healthcare Software") and HI Hub (the "HI Software")</li> <li>The parties have agreed to the supply, hosting, access and sharing of applicable personal data in accordance with the terms and conditions of this Agreement and under the governance of the <b>Data Sharing Framework</b>.</li> <li>Once this Contract Sheet is in agreed form and has been signed by the Participant, and CHIS Provider for the South West, the parties will have a binding contract incorporating the attached terms and conditions. The Participant shall return its executed counterpart to Health Intelligence at the address specified below, following which a copy of the fully executed and dated Agreement will be sent to the Participant at the address above.</li> </ul>	
<b>Participant Code:</b>	909
<b>Organisation Name:</b>	Bristol City Council
<b>Clients:</b>	NHS England South (South West)
<b>HI Address:</b>	Support Services, Health Intelligence Limited, Saxon House, Moston Road, Sandbach, Cheshire, CW11 3HL

<b>SIGNATURE</b>		
We confirm that we have read and agree to the terms and conditions attached below including the Schedules and Data Processing Contract.		
<p><b>Signed for and on behalf of the Participant:</b></p> <p><u>1) Director with responsibility for School Enrolment Data (relating to School-Aged Immunisations Provider (or deputy))</u></p> <p>Name: Sue Rogers</p> <p style="text-align: center;"></p> <p>Signature:</p> <p>Date: 7 September 2018</p> <p><u>2) Director with responsibility for Childhood Measurement Programme Service (or deputy)</u></p> <p>Name: Sue Milner</p> <p style="text-align: center;"></p> <p>Signature:</p> <p>Date: 7 September 2018</p> <p><u>3) Director with responsibility for Public Health Access (or deputy)</u></p> <p>Name: Sue Milner</p>	<p><b>Signed for and on behalf of the Participant:</b></p> <p>Name: Terry Dafter</p> <p>Signature:</p> <p style="text-align: center;"></p> <p>Caldicott Guardian/Information Governance Manager</p> <p>Date: 7 September 2018</p>	<p><b>Signed for and on behalf of the South West CHIS</b></p> <p>Name: Phil Kirby</p> <p>Signature:</p> <p style="text-align: center;"></p> <p>Philip Kirby, Managing Director Health Intelligence Ltd</p> <p>Date: <u>12/09/2018</u></p>

**THE PARTIES AGREE AS FOLLOWS:****1 DEFINITIONS**

1.1 In this Agreement, the following expressions shall have the following meanings:

<b>“Agreement”</b>	Means the Contract Sheet and these terms and conditions
<b>“Audit”</b>	Has the meaning given to it in Clause 5.8
<b>“Contract Sheet”</b>	Means the completed and executed contract sheet preceding these terms and conditions.
<b>“Client”</b>	Means the NHS organisation, which has contracted with HI for the provision of the Service as specified in the Contract Sheet.
<b>“Business Functions”</b>	Means the Participant’s functions characterised within the SCHEDULE 3 (examples being “Clinical care provision”, or “Screening /appointment administration”).
<b>“CHIS”</b>	Child Health Information Service
<b>“CHIS Provider”</b>	Health Intelligence Ltd for the period commencing 1 <sup>st</sup> April 2018.
<b>“Contract”</b>	Means the agreement entered into between the Client and Health Intelligence for the provision of the South West CHIS.
<b>“Data Processing Contract”</b>	A contract between the Participant and the CHIS Provider for the South West (see Appendix A)
<b>“Data Protection Legislation”</b>	Means, until 25 May 2018, the Data Protection Act 1998 and from 25 May 2018 onwards the General Data Protection Regulation and Data Protection Bill (as enacted in UK law) , and where <b>“Data Controller”</b> , <b>“Data Processor”</b> , <b>“Data Subject”</b> , <b>“Personal Data”</b> , <b>“Process”</b> or <b>“Processing”</b> are referred to in this Agreement, they shall have the meaning specified in the Data Protection Legislation.
<b>“Field Sets”</b>	Identify the range of care settings (primary care, outpatient care, inpatient care, welfare) and accompanying data which may be accessed by the Participant to perform its Business Functions appropriately.
<b>“Data Sharing Framework”</b>	The South West CHIS Data Sharing Framework. The Framework is required to be in place prior to this Sign-up Document being placed in agreed form.
<b>“FOIR”</b>	Means a request under the Freedom of Information Act 2000.
<b>“General Data Protection Regulations” or “GDPR”</b>	The regulations being adopted by the UK Government relating to the General Data Protection Regulations (GDPR) being enacted during May 2018 and placing additional obligations on organisations regarding transparency, fair processing and additional rights for the data subject.
<b>“Health Intelligence Ltd”</b>	Means Health Intelligence Ltd, the organisation contracted to provide the CHIS from 1 <sup>st</sup> April 2018 for an initial term of 5 years.
<b>“HI”</b>	Means Health Intelligence Ltd, the organisation contracted to provide the CHIS from 1 <sup>st</sup> April 2018 for an initial term of 5 years.
<b>“HI Software”</b>	Has the meaning given to it in the Contract Sheet. HI software will collate personal data from General Practice and feed updates to CarePlus; it will also provide enhanced report in support of the CHIS.
<b>“Participant”</b>	The organisation who is a party to this Agreement.
<b>“Personal Data Sets”</b>	Means the Participant’s personal data (for current patients registered with the Participant) held on its clinical system, as specified in SCHEDULE 1 (and as may be extended by the agreement of the parties from time to time).
<b>“Record Set Restrictions”</b>	Means the parameters limiting the views that the Participant and/or its authorised users may have based upon Personal Data, eg “Current patients”, “referred/awaiting review”, “and alive”, “anonymised trend summary” as specified in SCHEDULE 3.
<b>“Security Manager”</b>	Means the individual within the organisation who takes ownership of information security /information governance matters.
<b>“Security Officer”</b>	Means the party appointed as such by the Participant, as required by the Security Policy.
<b>“Security Policy”</b>	Means the Department of Health’s Information Security Management: NHS Code of Practice (2007) and any specific procedures established by the SW CHIS IG Sub-Group on behalf of all participants in respect of security, confidentiality and patient consent obligations, as made available to the applicable participants from time to time.
<b>“Service”</b>	Has the meaning given to it in the Contract Sheet.
<b>“Support Desk”</b>	Means HI’s support desk in respect of the HI Software, contactable by Participants via email through <a href="mailto:supportdesk@health-intelligence.com">supportdesk@health-intelligence.com</a> or via telephone on (01270) 527 373.
<b>“System C Healthcare Software”</b>	System C Healthcare Ltd provides a browser-based Child Health Information System (CHIS) known as CarePlus. One instance for the whole of the South West is being deployed. It will be hosted by System C Healthcare in their secure data centre. Health Intelligence as the CHIS Provider and Data Processor, will manage System C’s delivery of the CarePlus in compliance with the Health Intelligence’s agreements with Data Controllers in Common.



- 1.2 In this Agreement, unless the context otherwise requires: (a) words in the singular include the plural and words in the plural include the singular and a reference to one gender shall include a reference to the other genders; (b) Clause, Schedule and paragraph headings shall not affect the interpretation of this Agreement; (c) the Schedules form part of this Agreement and shall have effect as if set out in full in the body of this Agreement and any reference to this Agreement includes the Schedules; (d) references to Clauses and Schedules are to Clauses and Schedules of this Agreement and references to paragraphs are to paragraphs of the relevant Schedule; (e) a **person** includes a natural person, corporate or unincorporated body (whether or not having a separate legal personality); (f) references to any enactment, order, regulation or other similar instrument shall be construed as a reference to the enactment, order, regulation or instrument as amended or re-enacted by any subsequent enactment, order, regulation or instrument; and (g) any words following the terms **including, include, in particular, for example** or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding such terms.

## 2 SUPPLY OF DATA

### 2.1 The Participant shall:

- 2.1.1 Share Personal Data Sets from the Participant's clinical system(s) using the most appropriate method over the N3/HSCN network in accordance with the provisions of this Agreement and the Security Policy (the data export method is expected to change over time).
- 2.1.2 Address any queries or data quality issues with the CHIS Provider.

### 2.2 The Participant hereby agrees to:

- 2.2.1 The data export of the Personal Data Sets to the CHIS Provider for the purposes of this Agreement
- 2.2.2 Ensure that it has complied with the DPA and GDPR regarding fair and lawful processing information, to support the supply, export and hosting of the Patient Data Sets to the CHIS Provider for the South West pursuant to Clause 2.2.1 above
- 2.2.3 The CHIS Provider arranging for the hosting the patient's personal data within the Service using System C Healthcare Ltd.'s Child Health Information System, known as CarePlus and on the Service.
- 2.3 Any extension to the content of the Personal Data Sets to be provided to the CHIS Service shall be agreed in writing between the parties, in the form of an addendum to this Agreement. The Participant or the CHIS Provider shall submit a written request to the other Party for any such extension and no such extension shall be effective or implemented until written confirmation is received.
- 2.4 The Participant warrants that the Personal Data supplied by it to the Service was obtained by the Participant and provided to the CHIS Provider HI in compliance with the Data Protection Legislation.

## 3 DATA SHARING

- 3.1 Subject to Clause 3.2, the CHIS Provider shall be entitled to access and use the Personal Data Sets for the purposes of complying with its obligations under this Agreement and in supporting and providing the Service (SW CHIS).





- 3.2 Subject to Clause 3.3, the Participant hereby agrees to grant access to use the Personal Data Sets to the third parties identified in SCHEDULE 2 for the purposes set out therein. The CHIS Provider shall comply with the provisions of this Agreement and the Security Policy in respect of any sharing of the personal data pursuant to this Clause 3.1.
- 3.3 No access shall be granted to the Personal Data Sets pursuant to Clause 3.2 above unless:
- 3.3.1 An agreement to appropriately control access to the data and restrict user accounts to relevant healthcare and social care professionals has been entered into by the CHIS Provider with the applicable NHS or Social Care organisation identified in SCHEDULE 2.
  - 3.3.2 The healthcare professional requiring access to the data is an authorised user of the Service.
  - 3.3.3 The sharing arrangements detailed in SCHEDULE 2 are supported by a legal basis or the patient in question has provided consent for the purposes of access and use of their Personal Data by healthcare professionals involved in their care.
  - 3.3.4 Such patient consents are logged within the HI/System C Healthcare Software's applicable consent register.
- 3.4 Any changes to or extension of the access granted pursuant to Clause 3.2 above shall be agreed in writing between the parties, in the form of an addendum to this Agreement. The CHIS Provider shall submit a written addendum to the Participant for any such extension and no such extension shall be effective or implemented until the signed addendum from the Participant has been received.

#### **4 ACCESS TO THE SOFTWARE**

- 4.1 As a participant of the Service, the Participant shall (and will ensure that any of its employees, officers, contractors, agents and authorised representatives shall) use the Service in accordance with the provisions set out in SCHEDULE 3 and the terms of this Agreement.
- 4.2 The Participant shall be entitled to access the Personal Data Sets contained within the Service for the purposes of reviewing their registered children's child health record (including any child health records for children who should be associated with their organisation, e.g. as a result of their address). The CHIS Provider shall facilitate the provision of and reporting on such data to the Participant.
- 4.3 The Participant agrees that any information obtained from the Service shall:
- 4.3.1 Only be disclosed to, and used by, users and employers who plan, govern and/or deliver healthcare or social care services under the directives of the Participant for its patients.
  - 4.3.2 Only be used for the benefit of the applicable patient within the care of the Participant that is the Data Subject of the information in question.
  - 4.3.3 Not be provided to any third parties so as to avoid the requirement of such third party entering into a data sharing agreement in respect of the Personal Data Sets.
- 4.4 The Participant hereby agrees to:
- 4.4.1 If applicable, assign those Business Functions, Field Sets and Record Set Restrictions detailed in SCHEDULE 3 to its employees, contractors, link workers and other users



- 4.4.2 Use all reasonable endeavours to ensure that the Client (or, if applicable, any of its assignees and/or successors) is not placed in breach of any of its obligations under the Contract by virtue of any act or omission by the Participant and/or any of its employees, officers, contractors, agents and authorised representatives
  - 4.4.3 Report any faults, issues or enhancement requests relating to HI Hub or CarePlus to HI's Support Desk
  - 4.4.4 Abide by the Security Policy and nominate a Security Officer and/or "Caldicott Guardian" to undertake the duties specified in the Security Policy
  - 4.4.5 Record and notify the CHIS Provider of all incidents capable of placing at risk or affecting the confidentiality, integrity and availability of data delivered to, via, or from the Service immediately upon such incidents occurring and to fully co-operate and liaise with the CHIS Provider's nominated Security Manager on all such incidents.
- 4.5 The parties agree to co-operate and assist each other in complying with any subject access request by a Data Subject or authorised requests under the GDPR.
- 4.6 The Participant acknowledges and agrees that, in the event the Client is required to respond to a Freedom of Information Request (FOIR) relating to aggregate only data, the CHIS Provider shall be entitled to support and assist the Client as reasonably necessary in providing a response.

## 5 DATA PROCESSING

- 5.1 The Participant and the CHIS Provider acknowledge and agree that, for the purposes of the Data Protection Legislation, the Participant along with other clinical service providers are Data Controllers and that Health Intelligence is a Data Processor and its sub-contractor System C Healthcare Ltd as the providers of the CHIS system (CarePlus) are a sub-Data Processors in respect of any Personal Data.
- 5.2 The Participant acknowledges and agrees that System C Healthcare will act as a sub-Data Processor for the purposes of this agreement. The CHIS Provider will not otherwise engage sub-Data Processors to act on its behalf without prior written agreement of the Participant, such approval not to be unreasonably delayed or withheld.
- 5.3 The CHIS Provider will, and will also ensure the same of System C Healthcare, only Process the Personal Data in accordance with the Participant's instructions from time to time and shall not Process the Personal Data for any purpose other than those expressly authorised by the Participant, which shall include for the purpose of carrying out its obligations under this Agreement and as detailed within its contract with NHS England South (South West), unless otherwise required by law in which case the CHIS Provider will inform the Participant of those obligations before such Processing takes place, unless the CHIS Provider is prohibited from so doing by the law on grounds of public interest.
- 5.4 Appendix A provides a "**Data Processing Contract**"; it confirms the specific obligations of both the Participant and the CHIS Provider in relation to their obligations under the Data Protection Legislation and forms part of this Agreement.
- 5.5 HI warrants that:
- 5.5.1 it shall process the Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments each with the force of law, and in accordance with the common law duty of confidentiality;
  - 5.5.2 having regard to the state of technological development and the cost of implementing any measures it shall, and shall ensure that System C Healthcare, take appropriate



technical and organisational measures against the unauthorised or unlawful processing of Personal Data and against the accidental loss or destruction of, or damage to, Personal Data to ensure a level of security appropriate to (i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and (ii) the nature of the Personal Data to be protected;

- 5.5.3 It will ensure that its employees and agents, comply with such measures and the Security Policy;
- 5.5.4 it will ensure that System C Healthcare are subject to the same obligations as set out in this Agreement;
- 5.5.5 it will, taking into account the nature of processing, assist the Participant in ensuring its compliance with Articles 32 to 36 of the GDPR;
- 5.6 The Participant acknowledges that HI is reliant on the Participant (along with other Data Controllers) for agreeing the extent to which HI is entitled to use and Process the Personal Data in support of child health services.
- 5.7 HI agrees to indemnify and keep indemnified and defend at its own expense the Participant against all costs, claims, damages or expenses incurred by the Participant or for which the Participant may become liable due to any failure by HI or its employees or agents to comply with any of its obligations under this Agreement.
- 5.8 Subject to providing all reasonable notice to HI, the Client (and/or its authorised representatives) shall be entitled on behalf of the Participant to oversee an audit by HI of its compliance with the requirements of this Clause 5 (an "Audit") where required by the Data Protection Legislation. HI will provide the Client and the Participant with evidence of its compliance. In the event the Client does not exercise its rights of Audit under this Clause 5.4, the Participant shall be entitled to exercise such right, subject to receiving written authorisation to do so from the Client.
- 5.9 HI shall notify the Participant promptly if it becomes aware of any unauthorised or unlawful processing, loss of, damage to or destruction of the Personal Data ("promptly" shall be construed by reference to the nature of the unauthorised or unlawful processing loss of, damage to or destruction of the Personal Data, and the time at which HI became aware of the same).
- 5.10 HI will keep a record of any processing of personal data it carries out on behalf of the Participant.
- 5.11 HI shall promptly comply with any request from the Participant requiring HI to amend, transfer or delete any inaccurate Personal Data.
- 5.12 If HI receives any complaint, notice or communication which relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation (as such compliance relates to this Agreement) and the data protection principles set out therein, it shall promptly notify the Participant and it shall provide the Participant with co-operation and assistance in relation to any such complaint, notice or communication.
- 5.13 At the Participant's request, HI shall provide to the Participant a copy of all Personal Data held by it in the format and on the media reasonably specified by the Participant.
- 5.14 HI shall not transfer the Personal Data outside the European Economic Area without the prior written consent of the Participant.
- 5.15 Except as specified by the terms of this Agreement HI may not authorise any third party or sub-contractor to process the Personal Data.
- 5.16 HI shall notify the Participant within two (2) working days if it receives a request from a Data

Subject for access to that person's Personal Data.

- 5.17 HI shall provide the Participant with co-operation and assistance in relation to any request made by a Data Subject to have access to that person's Personal Data.
- 5.18 HI shall not disclose the Personal Data to any Data Subject or to a third party other than at the request of the Participant or as provided for in this Agreement.
- 5.19 On termination or expiry of the Contract, HI shall, following any necessary migration of data to a third-party replacement provider (as may be required by the Client), destroy all Personal Data provided by the Participant pursuant to this Agreement.

## **6 HI EMPLOYEES**

- 6.1 HI shall ensure that access to the Personal Data is limited to:
  - 6.1.1 Those employees of HI and System C Healthcare who need access to the Personal Data to meet HI's obligations under this Agreement, and
  - 6.1.2 In the case of any access by any employee, such part or parts of the Personal Data as is strictly necessary for performance of that employee's duties.
- 6.2 HI shall ensure that all employees (including those of System C Healthcare):
  - 6.2.1 are informed of the confidential nature of the Personal Data; and
  - 6.2.2 have undertaken training in the laws relating to handling Personal Data; and
  - 6.2.3 are notified of HI's and their own duties and obligations under this Agreement.
- 6.3 HI shall take reasonable steps to ensure the reliability of any of HI's employees who have access to the Personal Data.

## **7 TERM**

- 7.1 This Agreement shall commence as specified in the Contract Sheet and shall continue until:
  - 7.1.1 The Contract has been terminated or expires; or
  - 7.1.2 HI has ceased to have any data of the Participant (including the Personal Data Sets) under its custody or control, whichever is the later.
- 7.2 Either party shall be entitled to terminate immediately if the other party commits any material breach of this Agreement and fails to remedy that breach within thirty (30) days' written notice of that breach (the thirty (30) day period only applies where a breach is capable of remedy – if it is incapable of remedy, this Agreement may be terminated by written notice immediately).
- 7.3 Either party shall be entitled to terminate this Agreement, without clause, provided 3 months written notice is provided.
- 7.4 Termination or expiry of this Agreement shall not affect any accrued rights or obligations of either party arising out of this Agreement.

## **8 LIMITATION OF LIABILITY**



- 8.1 Neither party shall exclude or limit its liability under this Agreement for:
- 8.1.1 Death or personal injury caused by its negligence
  - 8.1.2 Fraud or fraudulent misrepresentation
  - 8.1.3 Any liability pursuant to an indemnity granted under this Agreement.
- 8.2 The CHIS Provider shall not be liable whether in contract, tort (including for negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, for any loss of profits, loss of business, depletion of goodwill and/or similar losses, loss or corruption of data or information, pure economic loss, or any special, indirect or consequential loss, costs, damages, charges or expenses however arising under this Agreement.
- 8.3 The Participant agrees that it will have no remedy in respect of any untrue statement or representation made to it (including those made negligently) upon which it relied in entering into this Agreement and that its only remedy can be for breach of contract (unless the statement was made fraudulently).
- 8.4 Each party's Contractual Liability to the other shall not exceed £10,000. "Contractual Liability" means the total liability howsoever arising under or in relation to the subject matter of this Agreement that is not (a) unlimited by virtue of Clause 8.1; or (b) excluded pursuant to Clauses 8.2 and 8.3.

## 9 CONFIDENTIALITY

- 9.1 Each party that receives ("**Receiving Party**") Confidential Information from the other ("**Disclosing Party**"), whether before or after the date of this Agreement shall: (a) keep the Confidential Information confidential; (b) not disclose the Confidential Information to any other person other than with the prior written consent of the Disclosing Party or in accordance with this Clause 9; and (c) not use the Confidential Information for any purpose other than the performance of its obligations or its enjoyment of rights under this Agreement ("**Permitted Purpose**").
- 9.2 The Receiving Party may disclose Confidential Information to its own officers, directors, employees, contractors, agents, and advisers who reasonably need to know such Confidential Information for the Permitted Purpose (each a "**Permitted Third Party**"), provided that the Receiving Party shall remain liable to the Disclosing Party for the acts, omissions, and compliance with the terms of this Clause 9 of such Permitted Third Party as if such Permitted Third Party was the Receiving Party (and a party to this Agreement). The Receiving Party shall ensure that each Permitted Third Party is made aware of and complies with all the Receiving Party's obligations of confidentiality under this Clause 9.
- 9.3 The terms of Clause 9.1 shall not apply to any information which: (i) is or becomes public knowledge other than by breach of this Clause 9; (ii) is independently developed without access to the Confidential Information; (iii) is in the possession of the Receiving Party prior to receipt from the Disclosing Party, other than by reason of a breach of this Clause 9 or any other obligation of confidence; or (iv) is received from a third party who lawfully acquired it and who is under no obligation restricting its disclosure.
- 9.4 If required by law, the Receiving Party may disclose Confidential Information to a court of competent jurisdiction or applicable regulatory authority or agency, provided that the Receiving Party shall (if legally permissible) provide reasonable advance notice to the Disclosing Party and co-operate with any attempt by the Disclosing Party to obtain an order providing for the confidentiality of such information to be maintained.



- 9.5 Neither party shall make any announcement or publicity statement relating to this Agreement or its subject matter without the prior written approval of the other party (except as may be required by law).

## 10 GENERAL TERMS

- 10.1 **Assignment:** Except for as provided in this Agreement, neither party shall assign, subcontract or otherwise transfer its rights or obligations under this Agreement in whole or in part without the prior written consent of the other party.
- 10.2 **No Waiver:** No failure or delay by either party to exercise any right, power or remedy shall operate as a waiver of that right, power or remedy nor shall any partial exercise preclude any further exercise of the same, or of any other right, power or remedy.
- 10.3 **Entire Agreement:** This Agreement supersedes any prior contracts, arrangements and undertakings between the parties in relation to its subject matter and constitutes the entire contract between the parties relating to the subject matter.
- 10.4 **Notices:** All notices and other communications under this Agreement shall be delivered by hand, courier, or first class pre-paid mail (either recorded delivery or registered) and will be deemed to have been served (i) if by hand, when delivered, or (ii) if by courier or first class pre-paid mail, forty-eight (48) hours after delivery to the courier or posting (as the case may be), provided that the parties may agree in writing to serve notices by fax and/or email. The addresses for service of notices under this Agreement shall be sent to the address of the recipient set out in the Contract Sheet, or to such other address as the recipient may have notified from time to time.
- 10.5 **Variation:** No variation of this Agreement shall be effective unless it is agreed by both parties in writing and signed by the parties' (or their authorised representatives).
- 10.6 **Severability:** Any provision of this Agreement which is held invalid or unenforceable shall be ineffective to the extent of such invalidity or unenforceability without invalidating or rendering unenforceable the remaining terms hereof.
- 10.7 **Remedies:** No right or remedy conferred by either party is exclusive of any other right or remedy contained in this Agreement or as any law may provide, but each shall be cumulative of every right or remedy given in this Agreement now or hereafter existing and may be enforced concurrently therewith or from time to time.
- 10.8 **Third Party Rights:** Except as expressly provided in this Agreement, the parties hereby exclude to the fullest extent permitted by law any rights of third parties to enforce or rely upon any of the provisions of this Agreement, whether pursuant to the Contracts (Rights of Third Parties) Act 1999 or otherwise.
- 10.9 **Relationship:** Nothing in this Agreement shall constitute or imply, or be deemed to constitute or imply, any partnership, joint venture, agency, fiduciary relationship or other relationship between the parties other than the contractual relationship expressly provided for in this Agreement. Nothing in this Agreement shall be deemed to constitute either party the agent of the other party, and neither party shall have, nor represent that it has, any authority to make any commitments on the other party's behalf.
- 10.10 **Counterparts:** This Agreement may be executed in any number of counterparts, each of which, when executed and delivered, shall be an original, and all the counterparts together shall constitute one and the same instrument.
- 10.11 **Jurisdiction:** This Agreement and any non-contractual obligations arising out of or in connection with it will be governed by English law and the parties irrevocably submit to the exclusive



jurisdiction of the courts of England for the determination of any dispute arising out of or in connection with this Agreement (including in relation to any non-contractual obligations).

- 10.12 **Dispute Resolution:** The parties to this agreement will work together to promptly resolve any dispute regarding the terms of this Agreement. NHS England South (South West) can be requested by either party to assist in the resolution of the dispute in the event that the parties cannot agree otherwise within 21 days.

**SCHEDULE 1**

**DATA SUPPLY & HOSTING**

**PERSONAL DATA SETS TO BE SUPPLIED BY THE PARTICIPANT**

**Table 1 – Personal Data Set, Content of the Export and Hosting Service**

**Please select only the relevant Data Exports**

Personal Data Sets	Personal Identifiable Data to be Shared and Hosted within the Service	
	Recommended Data Sets	Participant Confirmed
1. Maternity Department/Unit Data	<b>Note *1</b>	n/a
2. Newborn Blood Spot Screening Data	<b>Note *2</b>	n/a
3. Newborn Hearing Screening Data	<b>Note *3</b>	n/a
4. Health Visiting Service Data	<b>Note *4</b>	n/a
5. School Aged Immunisation Data	<b>Note *5</b>	✓
6. School Enrolment Data (School Lists)	<b>Note *6</b>	✓
7. Looked After Children Status Data	<b>Note *7</b>	✓
8. National Childhood Measurement Data	<b>Note *8</b>	n/a

\*1 The Maternity Department/Unit Data Flows are established flows of data to the CHIS, they include:

- Antenatal Assessments
- New Birth Notifications
- New Born & Infant Physical Examination (NIPE) data (Developmental checks)
- Discharge Data including BCG and Neonatal HepB Immunisations, screening for HepB positive status.
- Newborn Deceased Notifications and Pregnancy closures
- Looked After Child (LAC) or Safeguarding status information.

\*2 The Newborn Blood Spot Screening Data from the Blood Spot Laboratory is an established information flow to the CHIS. Screening Data to be provided to the CHIS is specified in a separate document; available upon request. Its relevance to those providing child health services is significant. Rare but serious health conditions can be identified using this screening programme and early treatment can improve their health and prevent severe disabilities and even death. The South West CHIS is responsible for sending out Newborn Blood Spot Screening Result Letters to Parents/Guardians.

\*3 Newborn Hearing Screening Data is an established information flow to the CHIS. It reports the results of hearing screening tests (typically 1-3 test results for each ear).

\*4 Health Visiting Service Data is an established information flow to the CHIS. It provides data from Health Visiting (0-19 year old) service providers including:

- Patient Registration Details – notifications of patients moving in an out of the Health Visiting Service area.





- \*5 School Age Immunisation Data is provided by School Age Immunisation Providers and is an established information flow to the CHIS. It details Pupil ID, NHS Number (where available), Administrative data and Vaccination status data.
- \*6 The Local Authority's Education Department shares school enrolment/list data with the CHIS. The Local Authority Public Health Department will not provide any data to the CHIS.
- \*7 The CHIS monitors the delivery of the Healthy Child Programme with a special emphasis on Looked After Children. The Local Authority shares details of this status with the CHIS.

A separate document details the specific data items that are being provided within these data flows. This document is not embedded as it is subject to change as the service develops, however it is available upon request.



**SCHEDULE 2  
DATA SHARING**

**Table 1 – Data Sharing Key:**

**PID** – Personal Identifiable Data;      **APD** – Anonymised Patient Data;      **AO** – Aggregate Only Reports may be accessed (numbers and percentages only).

Entries highlighted with **Bold** text form the current Data Sharing arrangements that will be established and maintained by HI Hub and CarePlus.

Access Matrix	General Practice			NHS England South (South West) (Client) i) Commissioning ii) Public Health *1			NHS Providers/ NHS Business Partners delivering Child Health Services *2			Local Authorities i) Public Health / ii) Education Departments *3			School Aged Immunisation Providers *4			Looked After Children & Safeguarding Teams *5		
	PID	APD	AO	PID	APD	AO	PID	APD	AO	PID	APD	AO	PID	APD	AO	PID	APD	AO
1. Administration Data for all Children aged 0 -18 years old inclusive (including deceased status)	<b>Yes</b>	n/a	<b>Yes</b>	i) No ii) <b>Yes</b>	No	<b>Yes</b>	<b>Yes</b>	No	<b>Yes</b>	i) No ii) <b>Yes</b>	No	<b>Yes</b>	<b>Yes</b>	No	<b>Yes</b>	<b>Yes</b>	No	No
2. New Born & Infant Physical Examinations NIPE) data (Developmental checks)	<b>Yes</b>	n/a	<b>Yes</b>	i) No ii) <b>Yes</b>	No	<b>Yes</b>	<b>Yes</b>	No	<b>Yes</b>	i) No ii) No	No	<b>Yes</b>	No	No	No	<b>Yes</b>	No	No
3. Bloodspot Screening Results	<b>Yes</b>	n/a	<b>Yes</b>	i) No ii) <b>Yes</b>	No	<b>Yes</b>	<b>Yes</b>	No	<b>Yes</b>	No	No	No	No	No	No	<b>Yes</b>	No	No
4. Childhood Vaccination & Immunisation data (including BCG and Neonatal HepB data)	<b>Yes</b>	n/a	<b>Yes</b>	i) No ii) <b>Yes</b>	No	<b>Yes</b>	<b>Yes</b>	No	<b>Yes</b>	i) No ii) No	No	<b>Yes</b>	<b>Yes</b>	No	<b>Yes</b>	<b>Yes</b>	No	No
5. Pregnancy Closures	<b>Yes</b>	n/a	No	i) No ii) No	No	No	<b>Yes</b> *6	No	No	i) No ii) No	No	No	No	No	No	No	No	No
6. Accident & Emergency Attendance	<b>Yes</b>	n/a	<b>Yes</b>	i) No ii) <b>Yes</b>	No	<b>Yes</b>	<b>Yes</b>	No	<b>Yes</b>	No	No	No	No	No	No	<b>Yes</b>	No	No

**Notes:**

**All organisation will be required to sign both the overarching Data Sharing Framework and a specific Data Sharing Agreement (similar to this agreement) to control their access to the personal data as reflected in this agreement.**

1. NHS England South (South West) as the Commissioners will be able to access Aggregate Only Data (Numbers and Percentages). Public Health England may access PID where there is a serious incident requiring investigation or as part of an audit request. Access will be restricted to relevant records only.
2. NHS Providers/NHS Business Partners under an NHS Contract to deliver Child Health Services include Health Visitor teams, School Nursing Teams, Acute (including Maternity Departments/Units), Newborn Bloodspot Laboratory, Newborn Hearing Screening Providers, Newborn Infant & Physical Examination (NIPE) providers, Vision Screening Providers, Mental Health and Community Health service providers who are engaged in delivering services to children. Each organisation will be required to sign both an overarching Data Sharing Framework and a specific Data Sharing Agreement to control their access to the patient data as reflected in this agreement. Looked After Children co-ordinators will also be able to access relevant patient data.
3. Local Authorities i) Public Health / ii) Education Departments. Public Health will be provided with access to Aggregate Only data. The Education Department will have access to administrative data only to confirm school enrolment and inform the School Age Vaccination Programme requirements.
4. School Age Immunisation Providers focus on the provision of school age vaccinations and the CHIS will facilitate the sharing of Administrative data to ensure all children are identified and their vaccination status is available in support of school health services.
5. Looked After Children (LAC) are supported to ensure they receive all the same Healthy Child screening elements and access to relevant child records will be provided to LAC teams (operating with commissioning or provider organisations). Safeguarding Teams will also be able to access the child health record for children under their review.
6. Pregnancy Closure status will be share with the relevant GP Practice and Health Visitor Team to prevent inappropriate visits.

Each organisation will be required to sign both an overarching Data Sharing Framework and a specific Data Sharing Agreement to control their access to the patient data as reflected in this agreement. Looked After Children co-ordinators will also be able to access relevant patient data.

**ePCHR:** the electronic version of the Red Book or Primary Child Health Record (PCHR) initiative is underway and will involve for authenticated and consenting parents/young adults, access to their child health data being provided securely via an electronic Red Book portal. The governance arrangements and consents to support this access will be obtained directly from the Parents/Young Adults following authentication. Provided robust authentication is in place, patients are entitled to access their health record data.

**Data Processors:** Health Intelligence (service provider of the South West CHIS and System C Healthcare are both Data Processors and as such personal data is not being shared with these organisations. Their hosting and processing of personal data is controlled by this Agreement and Health Intelligence's contracts with System C Healthcare for the provision of the CarePlus system and they have no rights to make use of the data they host and process for any other purpose.

### SCHEDULE 3

#### DATA ACCESS - Limitations on Use

**Table 1: The Service Business Purposes for the Participant**

The South West CHIS (Service) may be used by the Participant to support the business purposes detailed in the table below:

Business Purposes	Select by ticking the items
1. Provision of School Enrolment list verification	✓
2. Looked After Children Services and Safeguarding	✓
3. Public Health Oversight and Review	✓

**Table 2: Business Functions for the Participants**

Business Functions	Select by ticking the items
1. Maintaining an accurate register of children's school enrolment to ensure School-Aged Vaccination lists are accurate	✓
2. Monitoring Childhood Developmental Services for Looked After Children	✓
3. Public Health Population Health Review	✓
4. Commissioning of School-Aged Vaccination providers	✓
5. Provision of Failsafe and Safeguarding services for School-Aged children	✓

**Table 3: Field Sets for Participant**

The Field Sets identify the range of care settings (primary care, outpatient care, inpatient care, and welfare) and accompanying data that may be accessed to execute a Business Function appropriately.

Taken together with the Business Functions selected in Table 2 above, the Field Sets support the selection of data to be made available to different Participants. Individual users will be restricted within the specified range according to their function and role within the healthcare and social care provider community.

Field Sets	Select by ticking the items
1. Child Health Administrative Records	✓
2. Aggregate Data for Public Health Monitoring/Review	✓

**Table 4: Record Set Restrictions**

In respect of Table 4 below, Part A identifies the types of individuals (patients/clients) whose records the Participant would need to review. Part B identifies the level of detail that the Participant is empowered to view in accordance with the Data Protection Legislation and Health and Social Care Act (2012).

**Part A: Sets of patients for the Participant**

Set of Patients	Select by ticking the items
3. All Child Health Records associated with the area being served by the Participant.	✓



**Part B: Level of Access to Data**

Set of Patients	Select by ticking the items
1. Patient Identifiable Data for the Education Department	✓
2. Aggregate Only for the Public Health Department	✓

## APPENDIX A

# Data Processing Contract

## Issued under Article 28(3) of the General Data Protection Regulation

The Participant (hereinafter known as the Data Controller) and the CHIS Provider (hereinafter known as the Data Processor) are detailed on the Contract Sheet.

**Signature to the Contract Sheet confirms agreement to this Data Processing Contract.**

### BACKGROUND INFORMATION

- 1.1 The Data Processor is the CHIS Provider. The Data Processor has entered into a contract with NHS England South (South West) for the provision of the South West CHIS and is required to work with Data Controllers who deliver clinical services to children across the South West. The Participant to this Contract is a Data Controller.
- 1.2 The obligations within this Contract apply to both the Participant (as Data Controller) and the CHIS Provider (Data Processor).
- 1.3 Certain words and expressions used in and are applicable to this Contract are defined in the Definitions section (back page).

### DATA CONTROLLER RESPONSIBILITIES

- 2.1 The Data Controller is the data controller of the data insofar as it is Personal Data and, shall at all times, only Process Personal Data lawfully and in accordance with the General Data Protection Regulation ("GDPR") principles, as set out in Article 5.
- 2.2 It is the legal duty of the Data Controller to comply with, and be able to demonstrate compliance with, the data protection principles in relation to all Personal Data with respect to which he is a Data Controller (unless an exemption applies).
- 2.3 The Data Controller shall not instruct the Data Processor to Process Personal Data on his behalf under this Contract where the Data Controller does not have a lawful basis to Process that data.
- 2.4 The Data Processor is responsible for complying with this Contract and the GDPR in respect of the data processing it undertakes.
- 2.5 The data protection principles are set out in Article 5 of the GDPR. Article 28(3) requires that a number of specific legal stipulations are imposed on a Data Processor (and as set out below).

### DATA PROCESSOR RESPONSIBILITIES

- 3.1 The Data Processor shall Process Personal Data subject to the conditions set out in this Contract, and the further details of Processing in Schedule 1 of Appendix A.
- 3.2 The Data Processor shall:
  - 3.2.1 Process the Personal Data only in accordance with written instructions from the Data Controller to perform its obligations under this Contract;
  - 3.2.2 ensure that at all times it has in place appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data, including the measures as are set out in



Clause 4 below.

- 3.2.3 at all times Process the Personal Data in accordance with the Data Protection Legislation and the common law duty of confidence
- 3.2.4 not disclose or transfer the Personal Data to any third party or Data Processor personnel unless necessary and, for any disclosure or transfer of Personal Data to any third party, obtain the prior written consent of the Data Controller save where such disclosure or transfer is specifically authorised under this Contract or otherwise required by law. The Data Processor shall inform the Data Controller of any such transfers as soon as reasonably practicable, and not later than 3 Business Days after taking place;
- 3.2.5 take all reasonable steps to ensure the reliability and integrity of any Data Processor personnel who have access to the Personal Data and ensure that the Data Processor personnel:
  - a) are aware of and comply with the Data Processor's duties under this Clause, as well as its duties and obligations to ensure that the Personal Data is held securely and subject to a duty of confidence;
  - b) are informed of the confidential nature of the Personal Data, the duty of confidence which they owe to that Personal Data 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 Data Controller or as otherwise permitted by this Contract; and
  - c) have undergone adequate training in the use, care, protection and handling of Personal Data;
- 3.2.6 notify the Data Controller within 72 hours if it receives f from a Data Subject (or third party on their behalf):
  - a) a Data Subject Access Request (or purported Data Subject Access Request);
  - b) a request to rectify, block or erase any Personal Data;
  - c) any other request, complaint or communication relating to the Data Controller's obligations under the Data Protection Legislation;
  - d) any communication from the Information Commissioner or any other regulatory Data Controller in connection with Personal Data; or
  - e) a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;
- 3.2.7 only engage sub-processors to process Personal Data on its behalf with the express prior written consent of the Data Controller, and upon the same written contractual terms as set out in this Clause. The Data Processor will remain liable to the Data Controller for any breaches of the Data Protection Legislation committed by its sub-processors;
- 3.2.8 provide the Data Controller with full cooperation and assistance (within the timescales reasonably required by the Data Controller) in relation to any complaint, communication or request including by promptly providing:
  - a) the Data Controller with full details and copies of the complaint, communication or request;
  - b) where applicable, such assistance as is reasonably requested by the Data Controller to enable the Data Controller to comply with a Data Subject's Rights within the relevant timescales set out in the Data Protection Legislation; and



- c) on request by the Data Controller, any Personal Data it holds in relation to a Data Subject;
- 3.2.9 provide the Data Controller with full cooperation and assistance (within the timescales reasonably required by the Data Controller) in relation to any Data Protection Impact Assessment which the Data Controller is required to conduct in accordance with the Data Protection Legislation;
- 3.2.10 provide the Data Controller with full cooperation and assistance (within the timescales reasonably required by the Data Controller and taking into account the nature of the processing) to enable the Data Controller to comply with its obligations under the Data Protection Legislation;
- 3.2.11 inform the Data Controller immediately if asked to do something in respect of Personal Data which would constitute an infringement of the Data Protection Legislation;
- 3.2.12 delete all Personal Data at the cessation of this Contract or, if so instructed by the Data Controller, otherwise return all Personal Data to the Data Controller;
- 3.2.13 maintain an inventory detailing the Personal Data processed under this Contract, and the manner of this processing; and
- 3.2.14 if requested by the Data Controller, provide a written description of the measures that it has taken and technical and organisational security measures in place, for the purpose of compliance with its obligations pursuant to this Contract.

#### **Audit**

- 3.2.15 The Data Controller, and/or their appointed representatives (**Auditors**) shall be entitled to enter the Data Processor's and/or its sub-Data Processors' premises to inspect and audit the Data Processor's Processing of any Personal Data and take copies of relevant documentation (**Data Protection Audit**).
- 3.2.16 The Data Protection Audit shall only take place:
  - a) during the duration of the Contract;
  - b) not more than once in any calendar year;
  - c) on not less than 5 business days' prior written notice from, unless such Data Protection Audit is urgent, in which case on not less than 3 business days' prior written notice from the Data Controller; and
  - d) during ordinary business hours.
  - e) The Data Processor shall provide its full co-operation including, but not limited to, providing access to any of the Data Processor's premises and making appropriate personnel and facilities available to the Auditors and shall provide the Auditors with all reasonable assistance to enable such inspection, auditing and copying to take place.
  - f) Each party shall bear its own costs of the Data Protection Audit.
  - g) The Data Processor shall not Process or otherwise transfer any Personal Data in or to any country outside the European Economic Area or any country not deemed adequate by the European Commission pursuant to Article 25(6) of Directive 95/46/EC (together "**Restricted Countries**").
  - h) The Data Processor shall use its reasonable endeavours to assist the Data Controller to comply with any obligations under the Data Protection Legislation and shall not perform its obligations under this Contract in such a way as to cause the Data Controller to breach any of the Data Controller's obligations under the Data Protection Legislation to the





extent the Data Processor is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

## DATA SECURITY REQUIREMENTS

The Data Processor shall:

- 4.1 Have regard to the state of technological development and to the cost of implementing any measures, provide a level of security (including appropriate technical and organisational measures) appropriate to the harm that might result from unauthorised or unlawful processing of personal data or the accidental loss, damage or destruction of personal data and the nature of that personal data.
- 4.2 Ensure that access to personal data is limited to those employees of the CHIS Provider and System C Healthcare who need access to meet the Data Processor's obligations under this Contract.
- 4.3 Take reasonable steps to ensure the reliability of the Data Processor's personnel who have access to the personal data, which shall include ensuring that all staff and those of System C Healthcare engaged by the Data Processor understand the confidential nature of the personal data, and have received appropriate training in data protection prior to their use of the data, and have signed a written undertaking that they understand and will act in accordance with their Organisations and their responsibilities for confidentiality under the Contract.

The Data Processor shall ensure that:

- 4.5 It has properly configured access rights for its staff, including a well-defined starters and leavers process to ensure appropriate access control.
- 4.6 Suitable and effective authentication processes are established and used to protect personal data.
- 4.7 Personal data is backed up on a regular basis and that any back up data is subject to vigorous security measures as necessary to protect the availability, integrity and confidentiality of the data.
- 4.8 Robust and tested business continuity measures are in place to protect the confidentiality, integrity and availability of the Data Controller's personal data.
- 4.9 Data is transferred securely where it is essential to do so in relation to this Contract and, ensure data transferred electronically is encrypted to the higher of the international data encryption standards for healthcare and National Standards (this includes data transferred over wireless or wired networks, held on laptops, CDs, memory sticks and tapes).
- 4.10 Shall take reasonable steps to ensure the reliability of any employees who have access to the Personal Data.
- 4.11 Employees are not able to access the data remotely e.g. from home or via their own electronic device or internet portal other than through a secure electronic network and in accordance with organisational remote working policy. No data shall be stored in such devices.
- 4.12 Where instructed by the Data Controller to dispose of data it is disposed of securely and confidentially in accordance with the secure destruction requirements specified in section 8.



## SERIOUS INFORMATION BREACH INCIDENT, INCIDENT REPORTING AND DUTY OF CANDOUR

- 5.1 The Data Processor shall have procedures in place to monitor access and to identify unauthorised and unlawful access and use of personal data.
- 5.2 The Data Processor shall immediately report any information security incident related to the personal data subject to this Contract to the Data Controller and undertakes to also fully cooperate with the Data Controller's incident investigation requirements.
- 5.3 In so far as the Data Controller is responsible for the personal data, it is the Data Controller's responsibility to ensure that the incident is reported to the Information Commissioner and Data Subjects as required.
- 5.4 The Data Processor shall notify the Data Controller promptly (and in any event no later than 24 hours after discovery) if it becomes aware of any actual, suspected or threatened unauthorised exposure, access, disclosure, Processing, use, communication, deletion, revision, encryption, reproduction or transmission of any component of the Personal Data, unauthorised access or attempted access or apparent attempted access (physical or otherwise) to Personal Data or any loss of, damage to, corruption of or destruction of Personal Data (**Notifiable Data Protection Incident**).
- 5.5 Any such notification shall, as a minimum, include the following information:
- 5.5.1 the nature of the breach, including the categories and approximate number of Data Subjects and records concerned;
- 5.5.2 the contact at the Data Processor who will liaise with the Data Controller concerning the breach; and
- 5.5.3 the remediation measures being taken to mitigate and contain the breach.
- 5.6 In the event that any of the information specified within clause 5.5 is unavailable at the time of initial notification then it shall be provided as soon as reasonable available and without undue delay.

## PROCESS FOR AGREEING VARIATIONS

- 6.1 Any variation to the terms of this Contract shall be agreed in writing by the parties.

## DISPUTE RESOLUTION PROCESS

- 7.1 Both parties shall aim to resolve all disputes, differences and questions by means of co-operation and consultation. Should this fail, then the dispute resolutions process in the standard NHS Commissioning contract will be engaged – the conditions contained in GC8. Other terms of that contract will not be applicable in any way to this contract

## SECURE DESTRUCTION

- 8.1 NHS data is subject to legal retention periods and should not be destroyed unless the Data Processor has received specific instruction to do so from the Data Controller. Where data has been identified for disposal:



- 8.1.2 The Data Processor shall ensure that NHS information held in paper form (regardless of whether originally provided by the Data Controller or printed from the Data Processor's IT systems) is destroyed using a cross cut shredder or subcontracted to a confidential waste company that complies with European Standard EN15713.
- 8.1.2 The Data Processor shall ensure that electronic storage media used to hold or process NHS Information is destroyed or overwritten to current National Cyber Security Centre (NCSC) standards as defined at <https://www.ncsc.gov.uk/topics/cyber-strategy>
- 8.1.3 In the event of any bad or unusable sectors that cannot be overwritten, the Data Processor shall ensure complete and irretrievable destruction of the media itself.
- 8.1.4 The Data Processor shall provide the Data Controller with copies of all relevant overwriting verification reports and/or certificates of secure destruction of NHS information at the conclusion of the Contract.

## EXIT FROM CONTRACT

- 9.1 The Data Controller may terminate this Contract with immediate effect by written notice to the Data Processor on or at any time after the occurrence of an event that gives rise to an information security incident or otherwise poses a risk of non-compliance with the data protection principles.
- 9.2 In order to protect personal data, the Data Processor agrees:
  - 9.2.1 To store and process personal data securely and destroy it confidentially when it is no longer necessary and instructed by the Data Controller.
  - 9.2.2 To return to the Data Controller any personal data held at the end of the Contract, ensuring secure transfer, or to make arrangements for its secure disposal upon the instruction of the Data Controller.

## LIABILITY AND INDEMNITY

- 10.1 Without affecting its liability for breach of any of its obligations under the Contract, the Data Processor shall indemnify the Data Controller in full for costs, losses, charges, expenses it suffers arising out of the Data Processor's loss of NHS information or unauthorised or unlawful use of it whether arising in negligence or is otherwise a breach of this Data Processing Contract and including any fine imposed on the Data Controller by the Information Commissioner by way of civil monetary penalty under s55 of the Data Protection Act.

## FREEDOM OF INFORMATION

- 11.1 The Data Processor acknowledges that the Data Controller is subject to the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR).
- 11.2 The Data Controller may be statutorily required to disclose further information about the contracted service or the Contract itself in response to a specific request under FOIA or EIR, in which case:
- 11.3 The Data Processor shall provide the Data Controller with all reasonable assistance and co-operation to enable the Data Controller to comply with its obligations under FOIA or EIR.
- 11.4 The Data Controller shall consult the Data Processor regarding commercial or other confidentiality issues in relation to the Contract. However, the final decision about disclosure of information or application of exemptions shall rest solely with the Data Controller.

## SCHEDULE 1 OF APPENDIX A

The Data Controller wishes to engage the services of the Data Processor to process personal data on his behalf under the terms and conditions of this Contract for the purposes of:

<p><b>General description of purpose of use of the data</b></p> <p>Provision of the South West CHIS to enable the appropriate sharing of personal data in support of direct patient care for children across the South West.</p> <p>The CHIS Provider will maintain the child health record with data feeds from General Practice, child health service providers and will facilitate the sharing of this data with organisations and healthcare professionals directly involved in the care of the child. Aggregate and Anonymised Personal Data will also be shared in support of commissioning and service planning.</p>
<p><b>Data subjects</b></p> <p>Children aged 0-18 years old and older where they are known to have a special educational need (up to the age of 26) and their mothers/related parties.</p> <p>Mothers to be.</p>
<p><b>Data classes</b></p> <ol style="list-style-type: none"> <li>1. Administration Data for all Children aged 0 -18 years old</li> <li>2. New Born Bloodspot and New Born hearing data</li> <li>3. New Born &amp; Infant Physical Examinations data (Developmental checks)</li> <li>4. Childhood Vaccination &amp; Immunisation data</li> <li>5. Health Visitor Services Developmental checks</li> <li>6. HepB status for mothers and women who are pregnant</li> <li>7. Looked After Children and At-Risk Groups Status data</li> </ol>
<p><b>Key service elements</b></p> <p>CHIS Software (CarePlus)</p> <p>HI Hub Software</p>
<p><b>Special provisions (if any)</b></p> <p>n/a</p>

## DEFINITIONS

“Data Controller”	has the meaning given in the Data Protection Legislation;
“Data Processor”	has the meaning given in the Data Protection Legislation;
“Data Subject”	has the meaning given in the Data Protection Legislation;
“Data Subject's Rights”	A request by a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation in relation to his or her Personal Data;
“Data Protection Legislation”	(as applicable): (i) the Data Protection Act 1998 (ii) the Data Protection Act 2017 (once implemented); and (iii) from 25 May 2018 onwards, Regulation (EU) 2016/679, as well as, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all other applicable law in respect of data protection and data privacy including any applicable guidance or codes of practice that are issued by the Information Commissioner, Working Party 29 and/or the European Data Protection Board (and each of their successors);
“Personal Data”	personal data (as defined in the Data Protection Legislation) which is Processed by the Supplier or any Sub contractor on behalf of the Authority or a Central Government Body pursuant to or in connection with this Contract;
"Process"	has the meaning given in the Data Protection Legislation. 'Processed' and 'Processing' shall be construed in the same manner.
“Sub-contractor”	any third party with whom: (a) the Supplier enters into a Sub-contract; or (b) a third party under (a) above enters into a Sub-contract; or the servants or agents of that third party;
“Working Day”	any day other than a Saturday, Sunday or public holiday in England and Wales.

## DOCUMENT CONTROL

This page is provided to support version control and will detail all changes since this original version.

Version	Date	Changes made:
V6.0	8 <sup>th</sup> May 2018	Amended to ensure compliance with the General Data Protection Regulation (GDPR)  Note some version numbers skipped.
V5.1	12 March 2018	Original Version for the SW CHIS.