

# **Data Protection Impact Assessment**

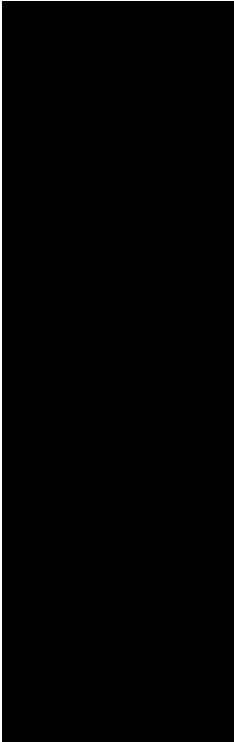
## **Population Health Management Sussex Integrated Dataset (SID)**

Document owner:	Sussex Health and Social Care Partnership
Document author and enquiry point:	Head of Information Governance and Data Protection Officer – Sussex Community NHS Foundation Trust on behalf of Sussex Health and Social Care Partnership
Review date of document:	3 <sup>rd</sup> June 2020
Version	Version 1 – 3 <sup>rd</sup> June 2020
Document File Name	SID DPIA V1 June 2020
Information Sharing Gateway Reference:	DS004500 DF006558

## Version History

Version	Status	Date	Summary of Changes
d0.1	Draft	05/11/2018	Initial Draft
d0.2	Draft	30/01/2019	Amended for SSID phase 1
d0.3 – 0.5	Draft	28/02/2019	Amended to support ISG workflow
d0.6 – 0.11	Draft	29/07/2019	Amended to support IG feedback
d12	Draft	02/06/2020	Updated to include reference to 3 <sup>rd</sup> Party
V1	Final	02/06/2020	Updated from ICS IG Steering Group consultation

## Reviewers

Name	Date	Title/Role
	28/02/2020	Data Protection Officer, East Sussex County Council, West Sussex County Council, Brighton and Hove City Council.
	09/03/2020	Group Head of Information Governance / Data Protection Officer, Brighton and Sussex University and Western Sussex Hospitals NHS Trusts
	03/03/2020	Operational Information Governance Lead, Brighton and Sussex University and Western Sussex Hospitals NHS Trusts
	03/03/2020	Information Governance Lead and Data Protection Officer, East Sussex Healthcare NHS Trust
	05/03/2020	Data Protection Officer, West Sussex County Council
	09/03/2020	GP IG and Data Protection Officer (DPO) for GP practices within the Sussex and East Surrey Alliance

## Requirement of for a Data Protection Impact Assessment (DPIA)

A DPIA must be completed wherever there is a change to an existing process or service or a new process or information asset is introduced that is likely to involve a new use or significantly changes the way in which personal data is handled to evaluate, in particular, the origin, nature, particularity and severity of that risk.

The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with the General Data Protection Regulations.

Following a DPIA, it may be necessary to use one of the following IG documents as part of the new project/processing:

- **Information Sharing Agreement** – This documents how information is shared with other organisation, including the purpose, legal justification/gateway and the details of the sharing required.
- **Data Processing Agreement / Contract** – This is used to record the responsibilities of the Data Controller and another organisation who may be employed as a Data Processor, to support a contract.
- **Data Transfer Agreement** – These are used to record the process and requirements for sending/receiving personal data with external organisations.

### **Appendices:**

*Appendix A: Definitions*

*Appendix B – Key Legislation and Guidance*

*Appendix C – Privacy Notices*

*Appendix D – Technical Information*

## Data Protection Impact Assessment - Part 1

This Data Protection Impact Assessment must be completed wherever there is a change to an existing process or service, or a new process or information asset is introduced that is likely to involve a new use or significantly changes the way in which personal data is handled.

<b>Title:</b>	Population Health Management Sussex Integrated Dataset		
<b>Lead manager:</b>			
<b>Name:</b>	Dan Hughes		
<b>Designation</b>	Programme Delivery Manager, Our Care Connected		
<b>Organisation</b>	Sussex Health and Care Partnership		
<b>Telephone</b>	07738 263999	<b>Email:</b>	dan.hughes2@nhs.net
<b>Overview: (Summary of the proposal)</b>	The Sussex Integrated Dataset (SID) is being established to support population health management in order to Improve the quality of health, well-being and care across Sussex Health and Care Partnership (SCHP).		
<b>Implementation Date:</b>	3 <sup>rd</sup> June 2020		

Screening Questions:			Yes/No
a.	<b>New collection/use</b>	Will the project involve the collection or processing of new information about individuals?	Y
b.	<b>Change of Purpose/s</b>	Are you planning to use information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Y
c.	<b>Information Sharing</b>	Will information about individuals be disclosed to organisations or people who have not previously had access to it?	Y
d.	<b>Privacy concerns</b>	Is the use of the information about individuals likely to raise privacy concerns or expectations?	N
e.	<b>Decision Making</b>	Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	N
f.	<b>Volume</b>	Does the project deal with significant volumes of records?	Y
g.	<b>Technology</b>	Does the project involve using or procuring new technology (including IT systems) or significantly changing current IT?	Y
h.	<b>Contractual</b>	Are services being contracted out to external organisations? (If so, a contract should be in place which contains relevant IG clauses to safeguard information)	Y
i.	<b>Contacting individuals</b>	Will the project require you to contact individuals in ways which they may find intrusive?	N
j.	<b>Identity</b>	Might the project have the effect of denying anonymity by sharing information that had previously been conducted anonymously into personal identifiable data?	N
k.	<b>UK Services</b>	Will the personal data be processed out of the U.K?	N

Screening Questions:			Yes/No
l.	<b>Automated decision making</b>	Will the project involve automated processing, including profiling, resulting in decisions that significantly affect individuals?	N
m.	<b>Genetic health data</b>	Will the project involved the collection of genetic health data?	N
n.	<b>IT Systems/ Electronic Records  (for IT Systems only)</b>	a) Will the project involve cloud service? b) Will the data be portable? (can it extracted and shared in a useable format) c) Can the data be permanently erased?	N Y Y
o.	<b>Decommissioning (IT Systems &amp; medical devices only)</b>	Will an IT system, or medical device, that stores personal data be decommissioned as part of this change?	N

The purpose of this assessment is to confirm that privacy laws and information governance standards are being complied with, or highlights problems that need to be addressed. It also aims to prevent problems arising at a later stage which might impede the progress or success of the project.

**Answering “Yes” to any of the screening questions above represents a potential IG risk factor that will have to be further analysed to ensure those risks are identified, assessed and fully mitigated.**

**If you have answered “Yes” to any of the questions above please proceed and complete Part 2**

## Data Protection Impact Assessment - Part 2

Data Processing	
1	<p><b>Is this a new or changed use/system of personal data that is already collected?</b></p> <p>New</p>
2	<p><b>Describe in as much detail why this data is being processed and the purpose of the project<sup>1</sup>?</b></p> <p>The Sussex Integrated Dataset (SID) is being established to improve the quality of health, well-being and care across Sussex Health and Care Partnership (SCHP).</p> <p>As defined by NHS England, and the NHS Long Term Plan, organisations within SHCP need to work as a whole system to ensure that the health and social care needs of the geography can be managed in a more coordinated way.</p> <p>Data processing is for the purpose of Research and Planning (Secondary uses / Indirect Care).</p> <p>There is an increasing need to share and link data between partner organisations within Sussex to ensure that system-wide modelling, analysis and monitoring can be effectively carried out to support better understanding of the connections and interdependencies between health and social care services and the patient flows between them, with the aim of improving patient outcomes by enabling closer collaboration, risk sharing and joint commissioning.</p> <p>Linking health and care data held across the system for people in Sussex with data on the wider determinants of health (including social characteristics and geographic patterns) to form broader population intelligence will support:</p> <ul style="list-style-type: none"> <li>• a greatly increased understanding of the existing use of health and social care services in Sussex, including the connections between different services;</li> <li>• a richer, system-wide view of the population's need for future health and social care services, looking across traditional organisational boundaries. This will provide new intelligence for a Sussex population health strategy;</li> <li>• the ability to understand variation through proactive benchmarking and comparison to improve clinical outcomes;</li> <li>• the ability to identify service improvements opportunities and financial efficiencies, for instance where patients use multiple services or where there is significant overlap between services;</li> <li>• public health intelligence work fulfilling statutory role of improving the health and wellbeing of people in Sussex, including Joint Strategic Needs Assessment, Health Needs Assessments, Health Equity Audits and Health Impact Assessments.</li> </ul> <p>Information will be shared by providers into the SID. This sharing does not include provider to provider sharing. Outputs of the SID will be available to providers.</p> <p><b>Future developments:</b> <i>The Sussex Integrated Dataset will be looking to include enhanced risk stratification and modelling to enable the re-identifying of information to GP practices in order support improvements to direct patient care.</i></p> <p><b>When this is model is available, a revised DPIA and Information Sharing Agreement</b></p>

<sup>1</sup> For example Direct Patient Care, Statistical, Financial, Public Health Analysis, Evaluation. See NHS [Confidentiality Code of Practice](#) Annex C for examples of use.

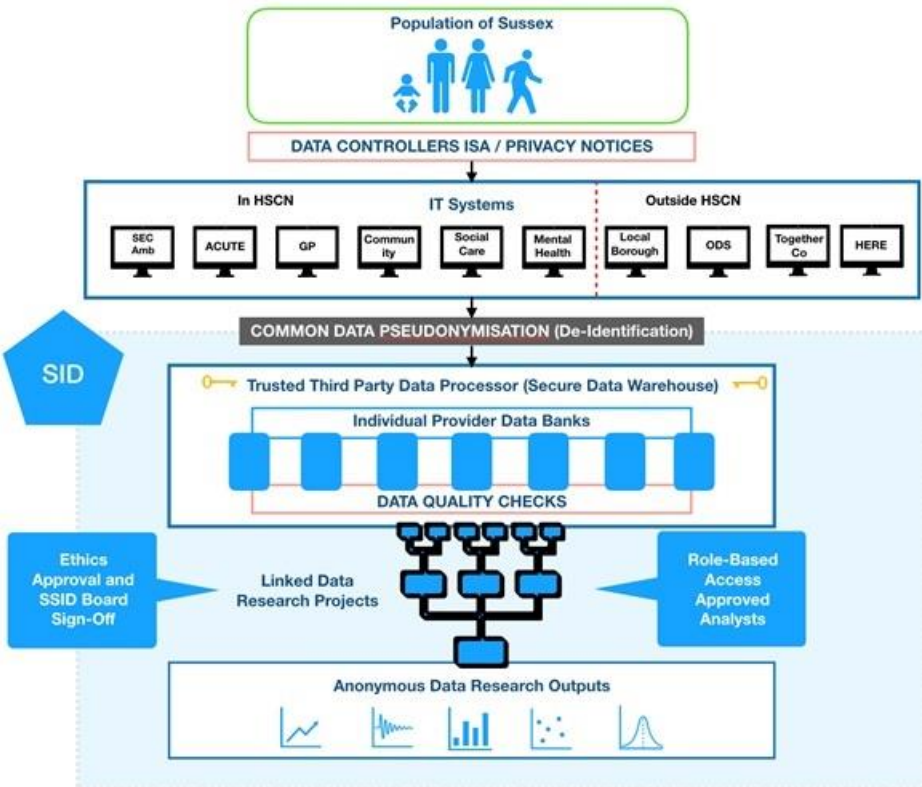
	<b>will be circulated for review and sign off.</b>																																								
<b>3</b>	<p><b>Does the processing actually achieve the purpose?</b></p> <p>Linked patient level data (pseudonymised) from health and social care providers within Sussex enables, analysts; researchers; public health consultants; doctors and health and social care professionals to have access to linked datasets in an anonymised format.</p> <p>This information can be used to understand more about disease risks and causes, improve diagnosis, develop new treatments and prevent disease, and to effectively improve and plan health and social care services with an aim to improve the local and individual care provided to patients.</p>																																								
<b>4</b>	<p><b>What data will be collected?</b></p> <table border="1"> <thead> <tr> <th>Personal Data:</th><th>Collected – Yes/No</th></tr> </thead> <tbody> <tr> <td>Forename:</td><td>N</td></tr> <tr> <td>Surname:</td><td>N</td></tr> <tr> <td>DoB</td><td>N</td></tr> <tr> <td>Age</td><td>Y</td></tr> <tr> <td>Gender</td><td>Y</td></tr> <tr> <td>Address</td><td>N</td></tr> <tr> <td>Postcode (Lower Super Output Area)</td><td>Y</td></tr> <tr> <td>NHS No</td><td>N</td></tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Special Categories</th><th>Collected – Yes/No</th></tr> </thead> <tbody> <tr> <td>Racial or ethnic origin</td><td>Y</td></tr> <tr> <td>Political opinion</td><td>N</td></tr> <tr> <td>Religious belief</td><td>Y</td></tr> <tr> <td>Trade Union membership</td><td>N</td></tr> <tr> <td>Physical or mental health or condition</td><td>Y</td></tr> <tr> <td>Sexual life</td><td>Y</td></tr> <tr> <td>Commission or alleged commission of an offence</td><td>N</td></tr> <tr> <td>Proceedings for any offence committed or alleged</td><td>N</td></tr> <tr> <td>Will the dataset include clinical data?</td><td>Y</td></tr> <tr> <td>Will the dataset include financial data</td><td>N</td></tr> </tbody> </table> <p><b>Other:</b> Pseudonymised NHS Number See Appendix D for full datasets</p>	Personal Data:	Collected – Yes/No	Forename:	N	Surname:	N	DoB	N	Age	Y	Gender	Y	Address	N	Postcode (Lower Super Output Area)	Y	NHS No	N	Special Categories	Collected – Yes/No	Racial or ethnic origin	Y	Political opinion	N	Religious belief	Y	Trade Union membership	N	Physical or mental health or condition	Y	Sexual life	Y	Commission or alleged commission of an offence	N	Proceedings for any offence committed or alleged	N	Will the dataset include clinical data?	Y	Will the dataset include financial data	N
Personal Data:	Collected – Yes/No																																								
Forename:	N																																								
Surname:	N																																								
DoB	N																																								
Age	Y																																								
Gender	Y																																								
Address	N																																								
Postcode (Lower Super Output Area)	Y																																								
NHS No	N																																								
Special Categories	Collected – Yes/No																																								
Racial or ethnic origin	Y																																								
Political opinion	N																																								
Religious belief	Y																																								
Trade Union membership	N																																								
Physical or mental health or condition	Y																																								
Sexual life	Y																																								
Commission or alleged commission of an offence	N																																								
Proceedings for any offence committed or alleged	N																																								
Will the dataset include clinical data?	Y																																								
Will the dataset include financial data	N																																								
<b>5</b>	<p><b>Quantity of records being used for this project**:</b></p> <p>The quantity of records will be based on the Sussex Health and Social Care Cohort 1.8 million people live in the Sussex Health and Care Partnership area (see <a href="https://www.england.nhs.uk/integratedcare/stps/view-stps/sussex-and-east-surrey/">https://www.england.nhs.uk/integratedcare/stps/view-stps/sussex-and-east-surrey/</a>)</p> <p>Data will be provided to the SID on a monthly basis by Sussex Health and Social Care Providers and quantity of records provided will be based on their own patient cohorts.</p>																																								

6	<p><b>Is there another way to achieve the same outcome?</b></p> <p>Not in this rich detail.</p>
7	<p><b>Organisations involved in processing the data?</b></p> <p>All organisations within the Sussex Health and Social Care Partnership will be asked to provide data into the SID and will become Joint Data Controllers. Providers of data will be indicated through sign up via the Information Sharing Gateway.</p> <p>East Sussex Healthcare Trust are the contracted Data Processors for the SID.</p> <p>The governance of the SID will be managed by the ICS Digital Programme Board and the ICS Information Steering Group in conjunction with the Data Controllers.</p>
8	<p><b>What is the legal basis for using the data under the General Data Protection Regulation 2016</b></p> <p><b>Article 6 - Lawfulness of processing:</b></p> <p>Article 6(1)(e) Performance of a public task</p> <p><b>What statutory power or duty does the Controller derive their official authority from?</b></p> <p>Health and Social Care Act 2012</p> <p><b>Article 9 - Processing of special categories of personal data</b></p> <p>Article 9(2)(h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional.</p>
9	<p><b>Are any of the data subject to a duty of confidentiality?</b></p> <p>Yes: Common Law Duty of Confidentiality</p>
10	<p><b>Describe the nature of the processing:</b></p> <p>The dataset will utilise patient-level data generated from Health and Social Care treatment episodes and interventions. Details will include: the nature and number of GP consultations, medical screenings and prescriptions; hospital admissions (including A&amp;E), duration of stay and aftercare; psychiatric and social care treatment episodes and community and social based interventions/prescribing.</p> <p>The information gathered will create a rich whole-population, anonymised person-level data platform for planning purposes aimed to improve intelligence, service improvements and patient outcomes.</p> <p>Data controllers will pseudonymise at source any datasets prior to sending to a trusted third party, who are under contract to process data for warehousing and linking.</p> <p>Once linked, the data can be queried to support service evaluation and design, evolution of public health intelligence, and return on investment estimation.</p> <p>Data Controllers will provide the fields included in an agreed data schema to a Trusted Third Party (TTP) Data Processor (herein called the Data Processor).</p> <p>A common pseudonymisation tool (PseudoApp) and training will be provided to each Data Controllers for local installation. The tool has been developed by Beautiful Information Ltd, a public/private organisation part owned by East Kent Hospitals University Foundation NHS Trust and Ashford and St Peters NHS Trust. It is a stand-alone tool that is downloaded on to</p>



	<p>a local computer at the data provider end. Each data provider is given a secure PIN login for the tool. Pre-defined data extract files (in .CSV format) are uploaded to the tool which then scans the files for initial data quality errors, then processes and automatically sends the data into the SID over a HTTPS connection. Beautiful Information does not have access to any Personal Identifiable Data.</p> <p>During the file processing, the tool will pseudonymise and encrypt any identifiable information at source: the NHS Number and date of birth are combined to create a unique patient pseudonym. Other processing carried out by the PseudoApp include transforming date of birth to become age, and address becomes lower super output area (i.e. typically containing 1,500 population) with a truncated post code. Local system patient identifiers and UPRN are encrypted.</p> <p>Where providers are using a third-party to provide data, e.g. CSU, it is the provider as Data Controller's responsibility to ensure they have appropriate contracts agreements in place for this data processing.</p> <p>The pseudonym is a hash computed using strong industry recognised algorithms (SHA256). It is never stored by the PseudoApp at source, but instead is created on the fly just prior to the transmission of data. These hashes are never available to the Providers. Once the data has passed through and been processed by the pseudonymisation tool it will be anonymous to anyone looking at it. When in this format the data will be securely transferred to the data processor.</p> <p>This process will recur on an agreed processing schedule (usually monthly) between the Data Controllers and the Data Processor.</p> <p>Data will be sent using a secure file transfer method using an API over HTTPS connection on the local N3 network. It will be stored by the Data Processor in a secure server provided by East Sussex Hospital Trust who are the contracted data processor.</p> <p>Row-level anonymised data access will be granted to approved data analysts under strict access controls, who will follow a common analytical method when querying the data. There is no fixed retention period as the data has value for longitudinal research.</p>
<b>11</b>	<p><b>What is the source of the data?</b></p> <p>Data will come from electronic patient administrative systems of primary and secondary health and social care data controllers within the Sussex Health and Care Partnership.</p>
<b>12</b>	<p><b>Where will the data be stored (physical or electronic location):</b></p> <p>Data will be stored electronically in the SID (Data Warehouse).</p> <p>East Sussex Healthcare Trust is the Data Processors hosting the SID.</p>
<b>13</b>	<p><b>Who will have access to the data? (list individuals or staff groups)</b></p> <p>The Data Analysts employed by the data processor will have access to pseudonymised data only.</p> <p>The data processor does not have access to the pseudonymisation 'key' therefore are unable to re-identify individuals.</p>
<b>14</b>	<p><b>Will you be sharing data with anyone?</b></p> <p>Information outputs from SID is anonymised, controlled and only authorised users can view.</p>
<b>15</b>	<p><b>Is there an ability to audit access to the data?</b></p> <p>Yes</p>

16	<p><b>Does this activity propose to use data that may be subject to or require approval from NHS Digital?</b></p> <p>No</p>
17	<p><b>What is the current state of technology in this area?</b></p> <p>The SID will use the latest standards in data pseudonymisation and anonymisation to protect the identity of patients.</p>
18	<p><b>Is there an approved Technical Assessment in place for any system(s) processing data:</b></p> <p>Yes. Approved by the Sussex Health and Social Care Partnership Digital Infrastructure Board on the 3<sup>rd</sup> June 2020</p>
19	<p><b>Are you proposing to use a third party/processor/system supplier as part of this project/activity?</b></p> <p>Yes:</p> <ol style="list-style-type: none"> <li>1) East Sussex Healthcare Trust</li> <li>2) Beautiful Information Ltd</li> </ol> <p><b>Has the third party met the necessary requirements under the GDPR and a contract in place?</b></p> <p>Yes:</p> <ol style="list-style-type: none"> <li>1) <b>East Sussex Healthcare Trust</b> <ul style="list-style-type: none"> <li>• Data Processing Contract in place</li> <li>• Data Protection Impact Assessment</li> <li>• Compliant to the Data Security and Protection Toolkit</li> </ul> </li> <li>2) <b>Beautiful Information Ltd</b> <ul style="list-style-type: none"> <li>• Contract in place with East Sussex Healthcare Trust on behalf of Sussex Health and Care Partnership.</li> </ul> </li> </ol> <p><b>Are there any ICO enforcement, decision notices, audit or advisory visit against the organisation?</b></p> <p>No</p>
20	<p><b>Are you transferring any data outside of the UK?</b></p> <p>No</p>
21	<p><b>Has a data flow mapping exercise been undertaken?</b></p> <p>Section 10 provides details of the nature of the processing. The following provides an overview of the processing which is supported by the technical documentation in Appendix D.</p>

	 <p>The diagram illustrates the data flow from the Population of Sussex to Anonymous Data Research Outputs. The process starts with the Population of Sussex, followed by Data Controllers ISA / Privacy Notices. Data is then split into 'In HSCN' (SEC Amb, ACUTE, GP, Community, Social Care, Mental Health) and 'Outside HSCN' (Local Borough, ODS, Together Co, HERE). This leads to Common Data Pseudonymisation (De-Identification), which feeds into a Trusted Third Party Data Processor (Secure Data Warehouse). The processor contains Individual Provider Data Banks and Data Quality Checks. The output is Linked Data Research Projects, which are then processed into Anonymous Data Research Outputs. The process is governed by Ethics Approval and SSID Board Sign-Off, and Role-Based Access Approved Analysts.</p>
<p>22</p>	<p><b>What security and audit measures have been implemented to secure access to and limit use of personal identifiable information?</b></p> <p>The use of personal data is limited by pseudonymising data at source.</p> <p>When data is sent to the Warehouse via the PseudoApp, patient identifiable data (NHS Number and DoB) is removed from the extracts and instead replaced with pseudo-identifiers (hash) for each patient. This hash is computed using strong industry recognised algorithms (SHA256). It is never stored by the PseudoApp at source, but instead is created on the fly just prior to the transmission of data. Therefore these hashes are never available to the Providers.</p> <p>In addition to this, other potentially identifiable information (local patient identifier, UPRN and Postcode) are encrypted using similarly strong algorithms prior to submission to the Warehouse.</p> <p>All installations of the PseudoApp will generate the same hash for a particular NHS Number and DoB combination as this functionality is fundamental to the linking of data in the Warehouse. Access to the Warehouse must be restricted and audited, available only to staff tasked with its development and maintenance.</p> <p>Although the Warehouse is receiving and storing these hashes, these are held internally to the Warehouse in the Landing and Processing databases and not available to the Providers or any Data Analysts in the Reporting database.</p> <p>The data warehouse has strict security measures and access controls in place (see Technical Assessment/Assurance).</p> <p>Access to data is secured using role-based access controls</p>

23	<p><b>Is Mandatory Staff Training in place for the following; Data Collection; Use of the System or Service; Collecting Consent (common law); Information Governance?</b></p> <p>Training will be provided to the providers in order to send data through the Pseudo Tool.</p> <p>All providers will need to be compliant with the Data Security and Protection Toolkit, which includes Mandatory Information Governance Training.</p>
24	<p><b>Will the process ensure the quality of the data being processed?</b></p> <p>Data supplied to the SID will be mapped and matched to a master SID data dictionary, to help maintain consistency of data. As data is supplied to the SID on a monthly basis, organisations have the capacity to correct previous errors in their latest submission. We will work closely with data providers, at dedicated data working groups, to understand data queries as they arise.</p>
25	<p><b>What assurances are in place for the decommissioning of any IT systems or medical devices? (IT systems &amp; medical devices only)</b></p> <p>Contractual. Any decommissioning of systems are managed through robust project management which includes what happens to the data.</p>
26	<p><b>What is the nature of your relationship with the individuals?</b></p> <p>Health and Social Care Patients and Service Users</p>
27	<p><b>How much control will individuals have over their processing?</b></p> <p>Data Controllers are individually responsible for ensuring their Privacy Notices (Fair Processing) include an explanation of their participation in the SID.</p>
28	<p><b>Would they expect you to use their data in this way?</b></p> <p>Data Controllers are responsible for informing their data subjects about their involvement in the SID.</p> <p>The SID Programme Board aims to engage patients and stakeholders to communicate its general purposes. The emphasis will be on explaining the social and personal benefits of health and social care analytics and research, being transparent and open about projects and activities, and explaining how ethical values are upheld, how individual privacy rights and freedoms are protected, and how we secure data.</p>
29	<p><b>Do they include children or other vulnerable groups?</b></p> <p>Data will include all patients within Sussex.</p>
30	<p><b>Are you aware of any existing concerns over the use of the data?</b></p> <p>No</p>
31	<p><b>What types of processing identified as likely high risk are involved?</b></p> <p>None – given that the pseudonymisation and linking processes (i.e. de-identifying the data and alignment of records between data controllers) have been performed appropriately under strict technical and contractual controls.</p> <p>Information outputs will be anonymised.</p>

Individuals Rights	
32	<p><b>Will patients be asked for consent (common law) for their information to be collected and/or shared?</b></p> <p>N/A: Only pseudonymised data is used within the SID and any only anonymised data is made available outside of the SID.</p>
33	<p><b>What changes are proposed to Fair Processing Notices of the organisations involved (Privacy Notices)?</b></p> <p>Organisations need to ensure that their privacy notices include information about the Population Health Management and the Sussex Integrated Dataset.</p>
34	<p><b>National Data Opt-Out</b></p> <p>The National Data Opt-out does not apply as this activity is not subject to Section 251 support. GPs should apply their Type 1 opt-outs prior to information being sent to SID.</p>
35	<p><b>Please set out the process for responding to requests under the right of access by data subjects.</b></p> <p>N/A – Each provider’s own processes will be in place</p>
36	<p><b>Please detail how this data will be made portable if requested by the data subject.</b></p> <p>N/A - Each provider’s own processes will be in place</p>
37	<p><b>Please detail how data subjects will be able to request the erasure of the data being processed. (Please see guidance for details on when this right is available).</b></p> <p>N/A - Each provider’s own processes will be in place</p>
38	<p><b>How long is the data/information to be retained?</b></p> <p>Only pseudonymised data will be held. There is no fixed retention period as it has value for longitudinal research or comparative analytics, e.g. service improvement over time.</p>
39	<p><b>How will it be possible to restrict the processing of personal data about a particular individual should this become necessary?</b></p> <p>Providers are able to remove individual patient’s details at source before provision to the SID.</p>
40	<p><b>If the organisation/service ceases what will happen to the data?</b></p> <p>Should a provider organisation cease, the information flow will cease and the provider closed off from the information sharing agreement.</p> <p>Where the data processor ceases, information will be transferred to an alternative data processor under contract, and the DPIA and Technical Assessment will be revised.</p> <p>Should the Sussex Integrated Data Set cease to exist, all held information will be securely deleted and the information sharing agreement closed off.</p>

41	<p><b>What plans are in place in relation to the internal reporting of a personal data breach?</b></p> <p>Data breaches will be regarded as serious and result in an investigation which may include disciplinary action.</p> <p>Each organisation is responsible for notifying other organisations to this agreement of any breach connected to the sharing of information under this Agreement. This obligation extends to breaches concerning the systems on which the data shared under this Agreement are held, even if the data shared under this Agreement is not directly affected.</p> <p>Organisations will agree an approach regarding onward reporting and investigation which can be facilitated through the ICS Information Governance Steering Group.</p>
42	<p><b>What plans are in place in relation to the notification of data subjects should there be a personal data breach?</b></p> <p>Should a breach occur which is in direct relationship to sharing under this assessment, organisations will agree an approach to the notification of data subjects.</p> <p>Each organisation is responsible for notifying the other organisation of any breach connected to the information described in this assessment. This obligation extends to breaches concerning the systems on which the data shared under this Agreement are held, even if the data shared under this assessment is not directly affected.</p> <p>Organisations will agree an approach regarding onward reporting and investigation which can be facilitated through the ICS Information Governance Steering Group.</p>
43	<p><b>Will any personal data be processed for direct marketing purposes? If yes please detail.</b></p> <p>No</p>
44	<p><b>Will the processing result in a decision being made about the data subject solely on the basis of automated processing (including profiling)?</b></p> <p>No</p>
<b>Risks, issues and activities</b>	
45	<p><b>What is the impact if the project/process does not go ahead?:</b></p> <p>The opportunity for improved patient care due to timely access to information of patients involved in shared care and multi-disciplinary teams will be lost.</p>
46	<p><b>How will you prevent function creep?</b></p> <p>There will be robust governance processes in place through the Sussex Health and Social Care Partnership Governance structures to ensure datasets and access is agreed.</p> <p>Any changes will be agreed through a formalised agreement and reviewed through the Sussex ICS Information Governance Group and where required a new DPIA completed.</p>
47	<p><b>Have any Information Governance risks been identified relating to this project?</b></p> <p>Yes, see Part 3</p>
48	<p><b>Is an Information Sharing Agreement required?</b></p> <p>Yes</p>

49	<p><b>Any further comments to accompany this DPIA that should be considered?</b></p> <p><b>Data Controller Statement</b></p> <p>For the purpose of the data within the Sussex Integrated Data Set, the providers of information will be considered as Joint Data Controllers.</p> <p>Article 26 of the GDPR States: Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, [Privacy Notices] by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.”</p> <p>The governance of the SID will be managed by the ICS Digital Programme Board and the ICS Information Steering Group in consultation with the Data Controllers.</p>
----	---

## Data Protection Impact Assessment - Part 3

Risk/s Identified and Action/s Required at Outset of Change/Project:

		Impact				
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Probability	Rare (1)	Low	Low	Low	Medium	Medium
	Unlikely (2)	Low	Low	Medium	Medium	Medium
	Possible (3)	Low	Medium	Medium	Medium	High
	Likely (4)	Medium	Medium	Medium	High	High
	Very Likely (5)	Medium	Medium	High	High	High

	Risk	Rating $P \times I = R$	Controls	Actions	Is the Risk at an accepted level?*
1	Processing is unlawful / Unfair	$2 \times 4 = 8$	Meets GDPR Legal Gateways DSPT compliance by all parties (including data processor) Existing fair processing and privacy notices Information security controls in place Data Minimisation through Pseudonymisation at source and anonymised outputs Data Processor Contract in place	Information sharing agreement Privacy Notices for programme	Yes



2	Individuals information related rights are not met	2 x 3 = 6	Meets GDPR Legal Gateways DSPT compliance by all parties Existing fair processing and privacy notices Information Security Controls in place	Information sharing agreement Privacy Notices for programme	Yes
3	Personal data is not held securely and an incident occurs	1 x 4 = 5	DSPT compliance by all parties (including data processor) Information security controls in place Data Minimisation through Pseudonymisation at source and anonymised outputs Pseudonymisation encryption key held securely outside of the providers and data processor. Existing fair processing and privacy notices Data Processor Contract in place	Technical Assessment completed and approved at Sussex Health and Care Partnership Infrastructure Board	Yes
4	Data quality issues with linked data	2 x 3 = 6	Incorporate data spot check procedures as part of the development to oversee and validate data linking. Data Minimisation through Pseudonymisation at source and anonymised outputs	Technical Assessment completed and approved at Sussex Health and Care Partnership Infrastructure Board	Yes
5	Pseudonymisation does not meet GDPR requirements	2 x 4 = 8	Information Security Controls in place Data Processor Contract in place	Technical Assessment completed and approved at Sussex Health and Care Partnership Infrastructure Board	Yes

6	'Small number' anonymised outputs (e.g. less than 5, or rare diagnoses) leading to 'accidental' identification of individuals	2 x 4 = 8	Small number suppression to be include in the criteria for anonymised outputs. Incorporate checking procedures in the data output processes.	Technical assessment for the data outputs	Yes
---	---	-----------	--	---	-----

*\*where the controls and actions are in place*

**Based on the information contained in this DPIA along with any supporting documents, the outcome is as follows:**

Agreed ensuring risks are managed accordingly.

**Please note:**

It is the responsibility of the Project/Activity Lead to notify the appropriate Information Asset Owner/Data Custodian/Information Asset Administrator for them to add to the Information Asset Register and Data Flow Mapping.

This DPIA will be disclosed if requested under the Freedom of Information Act (2000). If there are any exemptions that should be considered to prevent disclosure they should be detailed here:

## **Appendix A: Definitions**

Common Law Duty of Confidentiality	Common law requires there to be a lawful basis for the use or disclosure of personal information that is held in confidence.
Data Controller	A person who determines the purposes for which and the manner in which any personal data are, or are to be processed
Data Protection Impact Assessment (DPIA)	A documented process to identify and minimise the data protection risks.
Data Protection Officer	A data protection officer (DPO) is a role required by the General Data Protection Regulation (GDPR) and are responsible for overseeing an organisations data protection requirements to ensure compliance with GDPR requirements.
Direct Care	A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of an individual (all activities that directly contribute to the diagnosis, care and treatment of an individual).
Health Record / Clinical Record	A collection of clinical information pertaining to a patient's physical and mental health, compiled from different sources. Health records contain demographic data, next of kin, GP details, and most of the following: medical history; examinations; diagnoses; treatment; results of investigations, imaging; alerts and warnings; record of preventative measures; nursing records; clinical correspondence and referrals for treatment; discharge letters.
Health record system	The Electronic system used to store and manage a patient's clinical record.
legitimate relationship	The care relationship between a patient and a healthcare professional or group of healthcare professionals. It ensures that only care professionals involved in the patient's care can access the patient's clinical information.
Patient demographics	Details such as name, address, date of birth and NHS Number.
Privacy Notice	A statement made to a data subject that describes how an organisation collects, uses, retains and discloses

	personal information. A privacy notice is sometimes referred to as a privacy statement, a fair processing statement or sometimes a privacy policy.
Retention period	A retention period (associated with a retention schedule or retention program) is an aspect of records and information management (RIM) and the records life cycle that identifies the duration of time for which the information should be maintained or "retained," irrespective of format (paper, electronic, or other).

## Appendix B – Key Legislation and Guidance

The main legislation governing individuals' rights and relating to security and confidentiality that must be considered are:

Common law duty of confidentiality	Personal information held about families and children is subject to legal duty of confidence – not an absolute duty, but balance of public interest in maintaining confidentiality and public interest in disclosing the information
Computer Misuse Act 1990	Makes it an offence for any user to gain unauthorised access to information on a computer
Crime and Disorder Act 1998	Duty on all to prevent offending by children and young people; provides basic legal authority to disclose personal information where necessary to implement the act; promotes greater involvement of victims
Data Protection Act 2018	Sets new standards for protecting general data, in accordance with the GDPR, giving people more control over use of their data, and providing them with new rights to move or delete personal data.
Freedom of Information Act 2000	Individuals right of access to information
General Data Protection Regulation (GDPR) (2016)	Sets out the key principles for processing and sharing information. Individual's rights to confidentiality and security for their information and their right to access their own records.
Human Rights Act 1998	Article 8 – a right to respect for private and family life, with exception of public interest.
Regulation of Investigatory Powers Act 2000	Allows organisations to monitor automated communications e.g. email
The Heath Act 1999	States that NHS and local authorities shall cooperate with one another in order to secure the health and welfare of people (this allows practitioners to share information)

## **Appendix C – Privacy Notices**

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

Individuals must be provided with explanatory information including: the purposes for processing their personal data, retention periods, and who information will be shared with.

Privacy information must be provided to individuals at the time personal data is collected from them.

Where personal data is obtained from other sources, individuals must be provided with privacy information within a reasonable period of obtaining the data and no later than one month.

There are a few circumstances when people do not need to be provided with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.

The information provided must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

### **What should be included in a privacy notice?**

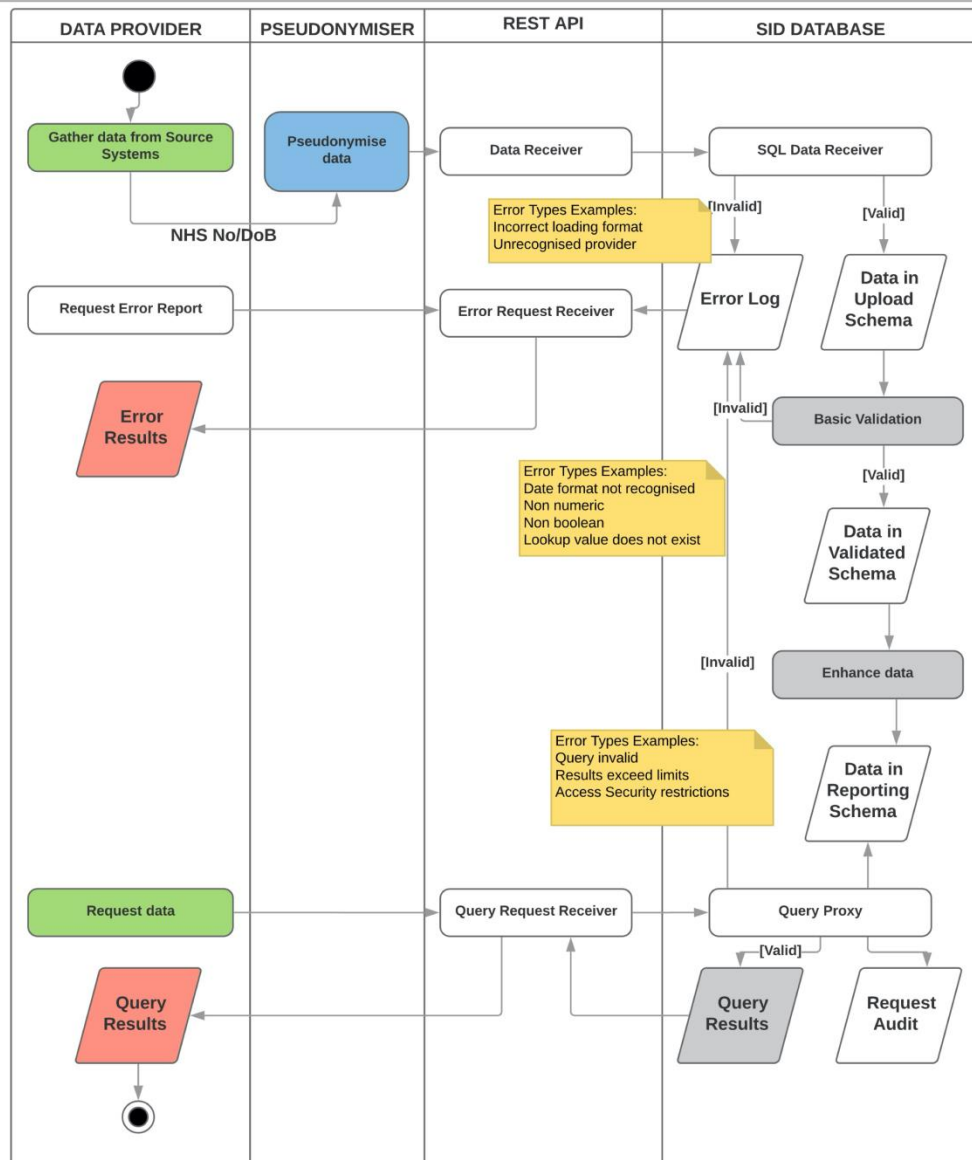
- The name and contact details of your organisation
- The contact details of your data protection officer
- The purposes of the processing
- The lawful basis for the processing
- The legitimate interests for the processing
- The recipients or categories of recipients of the personal data
- The details of transfers of the personal data to any third countries or international organisations
- The retention periods for the personal data
- The rights available to individuals in respect of the processing
- The right to withdraw consent
- The right to lodge a complaint with a supervisory authority
- The source of the personal data
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data
- The details of the existence of automated decision-making, including profiling

## Appendix D – Technical Documents

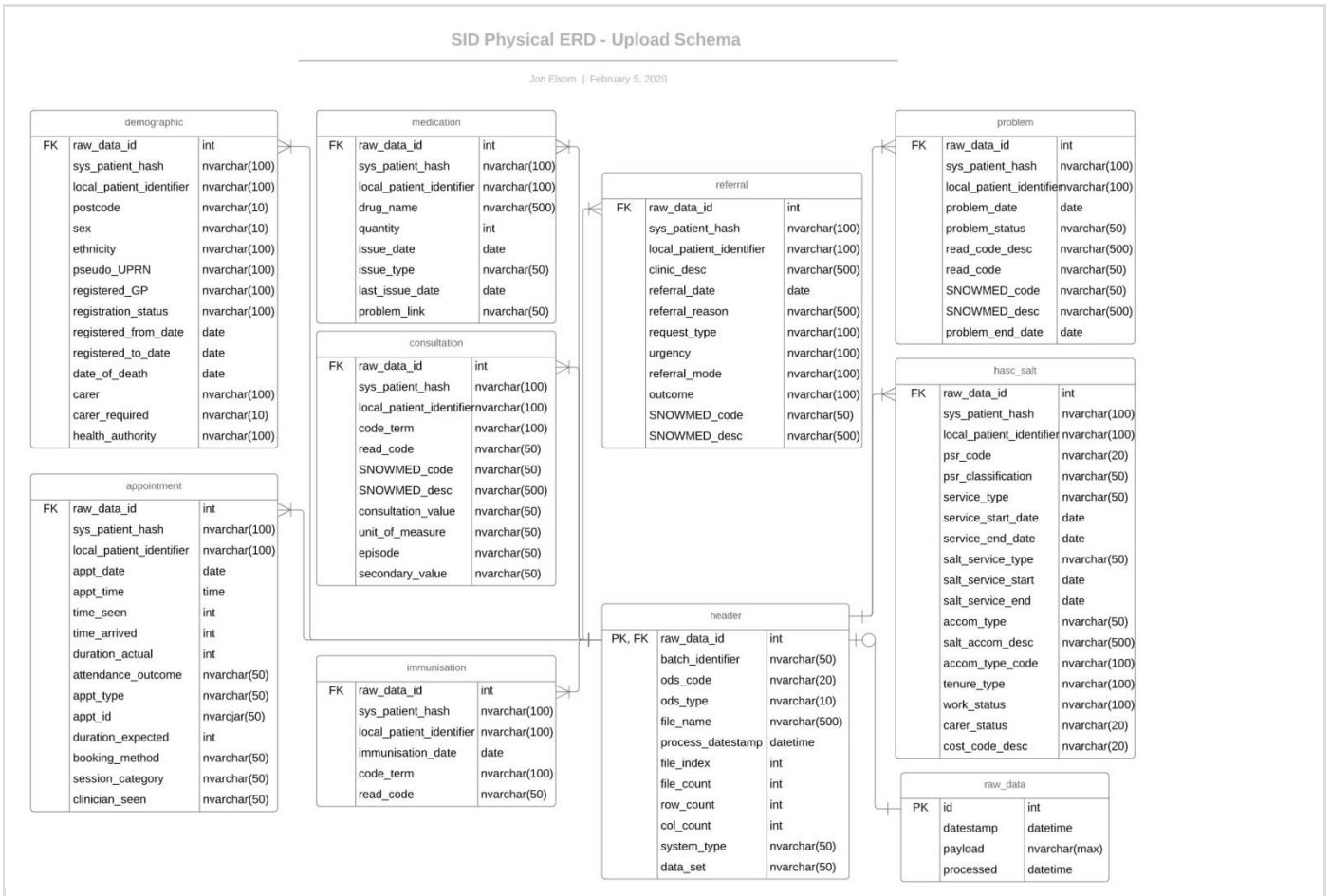
### DATA SCHEMA - v1.0

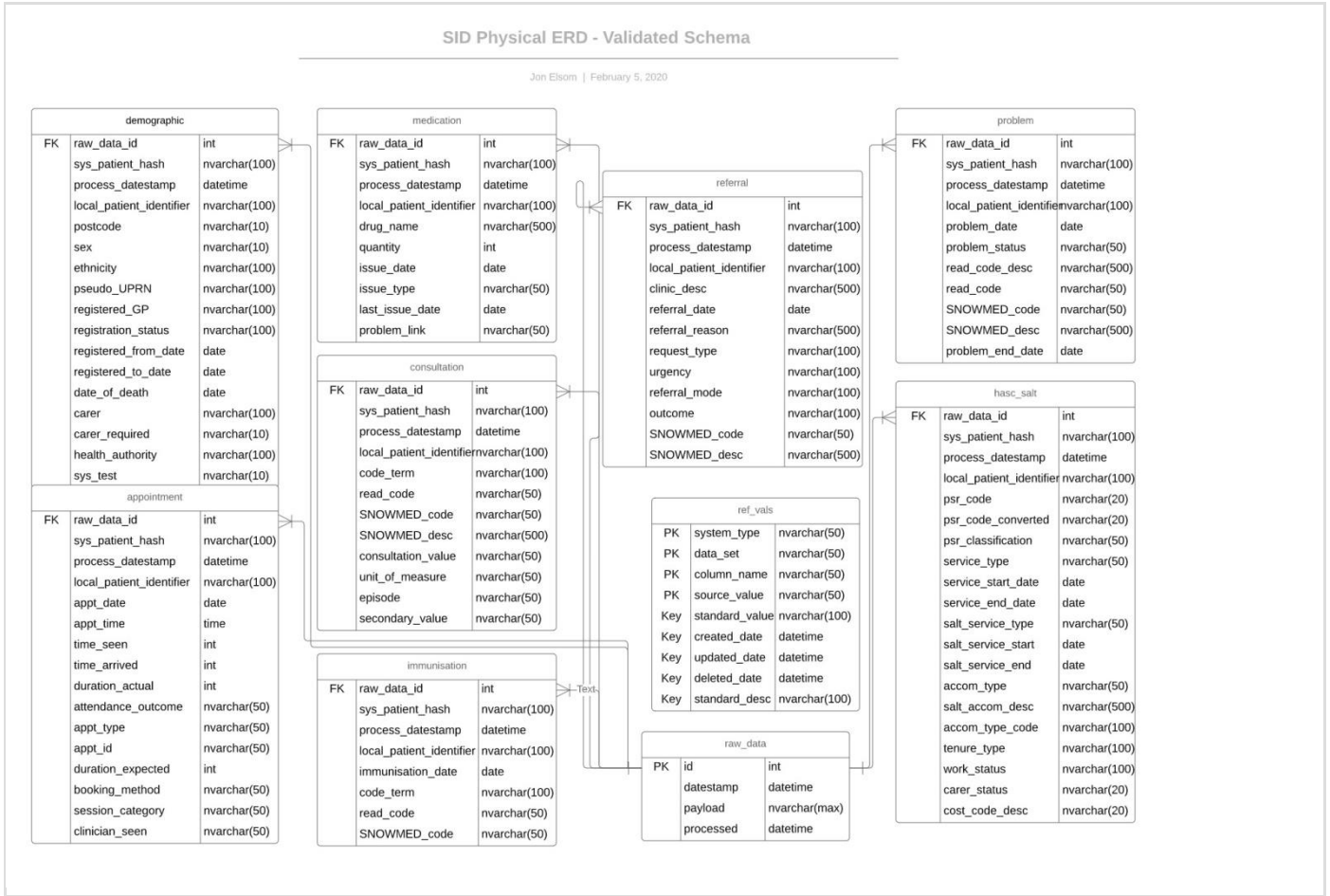
#### SID SWIM LANE ACTIVITY DIAGRAM LOADING AND QUERYING

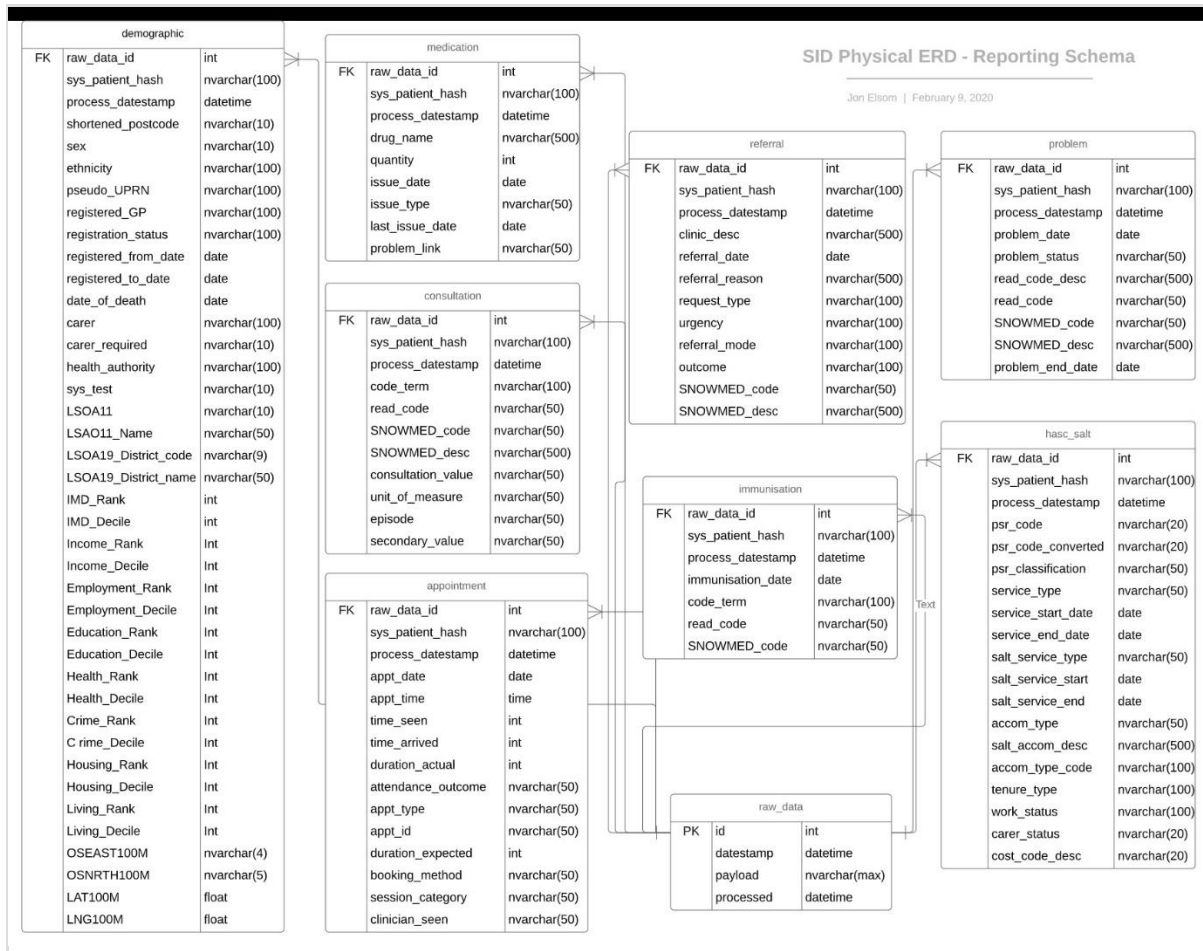
Jon Elsom | October 30, 2019











## DATA DICTIONARY

**A draft working copy of the SID Data Dictionary is available within the MS Teams Project Files: MS Teams Our Care Connected Site: [Click Here](#) or on request.**

## RESEARCH - DEMONSTRATION AREA RESEARCH QUESTIONS

1. Delaying permanent admissions to care homes: What opportunities can we identify through the use of linked data?  
Use of a logic model looking at factors amendable to change for:
2. Reducing hospital emergency admissions targeting those who have 2 or 5 more long-term condition
3. Improving life expectancy for those with mental illness, linking to management of physical and mental health conditions
4. Mental health / illness and health inequalities – understanding factors amendable to change
5. Evaluating cluster 6 integration pilot – measuring impact of multi-disciplinary working (we are going to set up before and after questionnaires, but it would be great to use the SSID if possible, for small numbers).
6. Self-management of multiple long-term conditions and factors that enable self-management and reduce interactions with primary and secondary care.
7. Uptake of cancer screening by key protected characteristics
8. Uptake of flu vaccinations by key protected characteristics
9. Improve the prevention, early detection and treatment of cardiovascular disease (CVD) and increase the numbers of people at risk of heart attack and stroke who are treated for the cardiovascular high risk conditions; Atrial Fibrillation, high blood pressure and high cholesterol.
10. NHS Checks Health Equity Audit

To use available data to assess the distribution of delivery of NHS Health Checks in Brighton & Hove among different population groups. Specific objectives:

- Assess the distribution of NHS Health Checks delivery in Brighton & Hove, by gender, age, ethnicity and IMD deprivation quintile.
- Determine whether groups with the highest CVD risk receive a greater proportion of NHS Health Checks.
- Describe the number of invitations, NHS Health Check delivery and number of referrals to other services in Brighton & Hove against targets holding question - NHS health checks impact on outcomes
- What is the effect of the NHS Health Check on disease detection, changing behaviours, referrals to local risk management services, reductions in individual risk factor prevalence, reducing CVD risk and on statin and antihypertensive prescribing?

Primary Care Network Questions:

Over the next couple of years we will need to have a system plan in place to improve the prevention, early detection and treatment of cardiovascular disease (CVD) and increase the numbers of people at risk of heart attack and stroke who are treated for the cardiovascular high risk conditions; Atrial Fibrillation, high blood pressure and high cholesterol.