Sussex
Health and Care Partnership

Data Protection Impact Assessment

‘Our Care Connected’
Sussex Shared Care Record

Document owner:	Sussex Health and 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 Care Partnership
Version	V1.0 November 2020
Document File Name	Direct Care DPIA V1 FINAL
Information Sharing Gateway Reference:	DS004770 DF007001

Version History

Version	Status	Date	Summary of Changes
d0.1	Draft	25/08/2020	Initial Draft
d0.2	Draft	16/09/2020	Amendments
d0.3	Draft	30/09/2020	Amendments
d0.4	Draft	30/09/2020	Amendments - for Consultation SHCP IG Group
d.05	Draft	26/10/2020	Final Review
V1	FINAL	26/11/2020	FINAL DOCUMENT

Reviewers

Name	Date	Title/Role
Heidi Judd	13/10/2020	Data Protection Officer, East Sussex County Council, West Sussex County Council, Brighton and Hove City Council.
Trudy Slade	14/10/2020	GP IG and Data Protection Officer (DPO) for GP practices within the Sussex and East Surrey Alliance
Richard Newell	19/10/2020	Independent Data Protection Officer
Andrew Harvey	20/10/2020	Group Head of Information Governance / Data Protection Officer, Brighton and Sussex University and Western Sussex Hospitals NHS Trusts
Ruth Paine	22/10/2020	Information Governance Lead and Data Protection Officer, East Sussex Healthcare NHS Trust
Katie Rees	10/11/2020	Head of Information Governance
Mark Vinten	10/11/2020	Delivery Lead and Technical Architect
Caroline Butler	10/11/2020	Digital Project Manager - Our Care Connected Programme

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 and UK Data Protection Act.

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

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.

Title:	‘Our Care Connected’ Sussex Shared Care Record		
Lead manager:			
Name:	Dan Hughes		
Designation	Programme Delivery Manager, Our Care Connected		
Organisation	Sussex Health and Care Partnership		
Telephone	[redacted]	Email:	[redacted]
Overview: **(Summary of the proposal)**	The ‘Our Care Connected’ Sussex Shared Care Record aims to improve the information that is available to health and care practitioners when managing patients and service users who are being cared for across multiple organisations to facilitate improved their health and care outcomes.		
Implementation Date:	November 2020		

Screening Questions:			**Yes/No**
a.	**New collection/use**	Will the project involve the collection or processing of new information about individuals?	Y
b.	**Change of Purpose/s**	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?	N
c.	**Information Sharing**	Will information about individuals be disclosed to organisations or people who have not previously had access to it?	Y
d.	**Privacy concerns**	Is the use of the information about individuals likely to raise privacy concerns or expectations?	N
e.	**Decision Making**	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.	**Volume**	Does the project deal with significant volumes of records?	Y
g.	**Technology**	Does the project involve using or procuring new technology (including IT systems) or significantly changing current IT?	Y
h.	**Contractual**	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.	**Contacting individuals**	Will the project require you to contact individuals in ways which they may find intrusive?	N

Screening Questions:			**Yes/No**
j.	**Identity**	Might the project have the effect of denying anonymity by sharing information that had previously be conducted anonymously into personal identifiable data?	N
k.	**UK Services**	Will the personal data be processed out of the U.K?	N
l.	**Automated decision making**	Will the project involve automated processing, including profiling, resulting in decisions that significantly affect individuals?	N
m.	**Genetic health data**	Will the project involved the collection of genetic health data?	N
n.	**IT Systems/ Electronic Records** **(for IT Systems only)**	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?	Y Y Y
o.	**Decommissioning (IT Systems & medical devices only)**	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	**Is this a new or changed use/system of personal data that is already collected?** This is a new shared care record system allowing integration between health and care systems in Sussex. In some cases this will be a new use of personal data but in others, there are already integrated system in place such as ROCI (Read Only Care Information) which is predominantly used across West Sussex and the Integrated Care Record (ICR) which is used across East Sussex. These platforms will be replaced by the Sussex Shared Care Record.
2	**Describe in as much detail why this data is being processed and the purpose of the project[1]?** The NHS Long Term Plan looks to upgrade technology and digitally enabled care where health and care practitioners can access and interact with patient and service user records and care plans wherever they are, with ready access to decision support without the administrative burden. Part of the Long Term Plan includes the Local Health and Care Record (LHCR) programme to create integrated care records across GPs, hospitals, community services and social care. ***Our Care Connected*** is the name for the Sussex LHCR. Putting the right information in the hands of health and care practitioners at the right time is an essential part of the provision of safe and effective care. When patients and service users are at their most vulnerable, providing health and care practitioners with access to a health and care record allows them to understand the individual needs and make the best decisions with the individual and support them in living independently at home and in their communities. The Sussex Shared Care Record is being developed to provide the ability to enable appropriate and effective sharing of information for direct care purposes, through the integration of current health and care record systems, to facilitate improved outcomes for patient and service users. Access to shared information is for the purposes of direct care by those who have a legitimate relationship with the patient or service user. Data controller organisations contributing data to facilitate the Sussex Shared Care Record, will be presented with one or more additional documents (e.g. DPIA, Data Specification Document, Technical Specifications), as part of the onboarding and change control processes which describe the organisational specific data requirements. Information governance assurance will be managed through the Sussex Health and Care Partnership Information Governance Steering Group. The associated Information Sharing Agreement(s), DPIAs and Data Flow information will be held on the Information Sharing Gateway© www.informationsharinggateway.org.uk. (see Appendix A: Definitions for further information). The Technical Specification and operation of this project will be updated throughout the length of the project as local technical approaches are developed and/or national guidance necessitates.

[1] For example Direct Patient Care, Statistical, Financial, Public Health Analysis, Evaluation. See NHS Confidentiality Code of Practice Annex C for examples of use.

Approval and technical assurance (including the security, safety and resilience) will be through the Infrastructure Standards Group, within the Our Care Connected assurance framework.

The standards to be applied are best practice and will be in keeping with industry best practice and approved by the Sussex Health and Care Partnership Infrastructure Standards Group.

3 Does the processing actually achieve the purpose?

Yes, The aim of the project is to achieve improvements in the safety and quality of care provided, in a technically safe and easy to use format (as defined in the Health and Care (Safety and Quality) Act, 2015).

Sussex currently does not have one single health and care information system across all organisations and therefore is not currently able to easily share information. Implementing an integrated system which links systems together ensures information is available at the right time, in the right place to the right practitioners.

4 What data will be processed?

Personal Data:	**Collected – Yes/No**
Forename:	**Y**
Surname:	**Y**
DoB	**Y**
Age	**Y**
Gender	**Y**
Address	**Y**
Postcode (Lower Super Output Area)	**Y**
NHS No	**Y**

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	**Y***
Proceedings for any offence committed or alleged	**Y***
Will the dataset include clinical data?	**Y**
Will the dataset include financial data	**N**

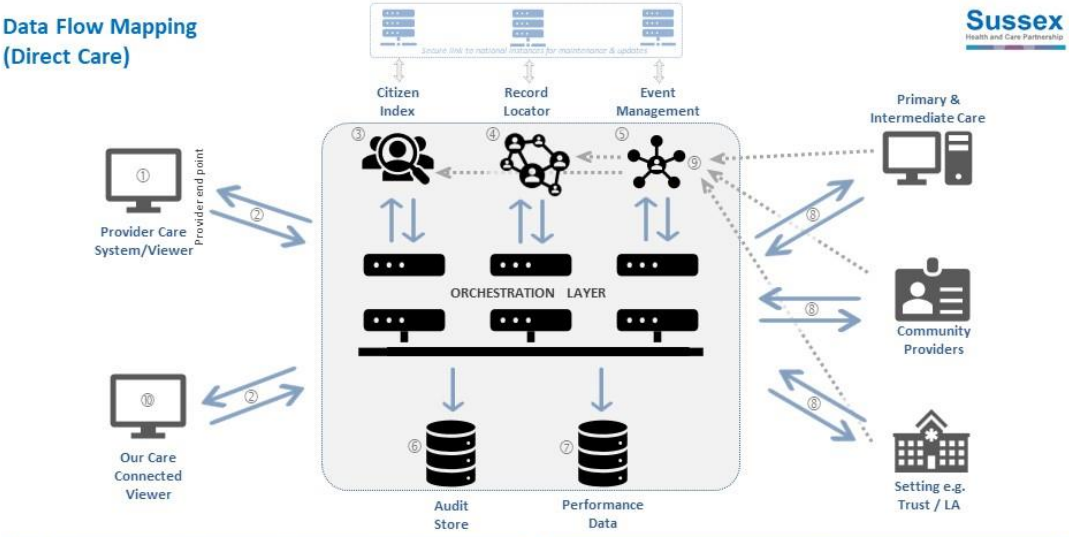
Providers will agree the specific datasets and technical configuration as part of the onboarding process, or as part of a change process to ensure the safeguarding of patient and service user information in line with the Technical Standards as set out by the SHCP Infrastructure Standards Group.

*only where safeguarding concerns are included, appropriate to share, and in line with Professional Records Standards Body (PRSB) Core Standards.

5	**Quantity of records being used for this project:** 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 https://www.england.nhs.uk/integratedcare/stps/view-stps/sussex-and-east-surrey/)
6	**Is there another way to achieve the same outcome?** Sussex could procure one system to develop a single shared care record, however the impetus to adopt one system is not there and would not meet the needs of different health and care providers across Sussex. Integration builds upon legacy systems, allows freedom of choice in the procurement of systems and data is held and maintained by the service providers.
7	**Organisations involved in processing the data?** All organisations within the Sussex Health and Care Partnership as detailed within the Information Sharing Gateway Reference: DS004770 and DF007001
8	**What is the legal basis for using the data under the General Data Protection Regulation 2016 and Data Protection Act 2018** ***GDPR Article 6 - Lawfulness of processing:*** Article 6(1)(e) Performance of a public task **What statutory power or duty does the Controller derive their official authority from?** Health and Social Care Act 2012 ***GDPR Article 9 - Processing of special categories of personal data*** 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.
9	**Are any of the data subject to a duty of confidentiality?** Yes: Common Law Duty of Confidentiality
10	**Describe the nature of the processing:** The Sussex Shared Care Record will draw health and care information from SHCP provider systems and will consist of demographic data (age, gender, address, NHS Number etc), medical information (diagnosis, issues/problems, medication, allergies, past medical history, pathology results), admission, discharge and transfer information, practitioner involvements, provisioned services and assessment information. Information is in line with the Professional Records Standards Body (PRSB) Core Standards. Data controller organisations that contribute data to the a data flow or information assets to facilitate the Sussex Shared Care Record, will be presented with one or more additional documents (eg DPIA, Data Specification Document, Technical Specifications) describing each specific processing and sharing arrangement the controller is expected to contribute to as part of their on-boarding process.

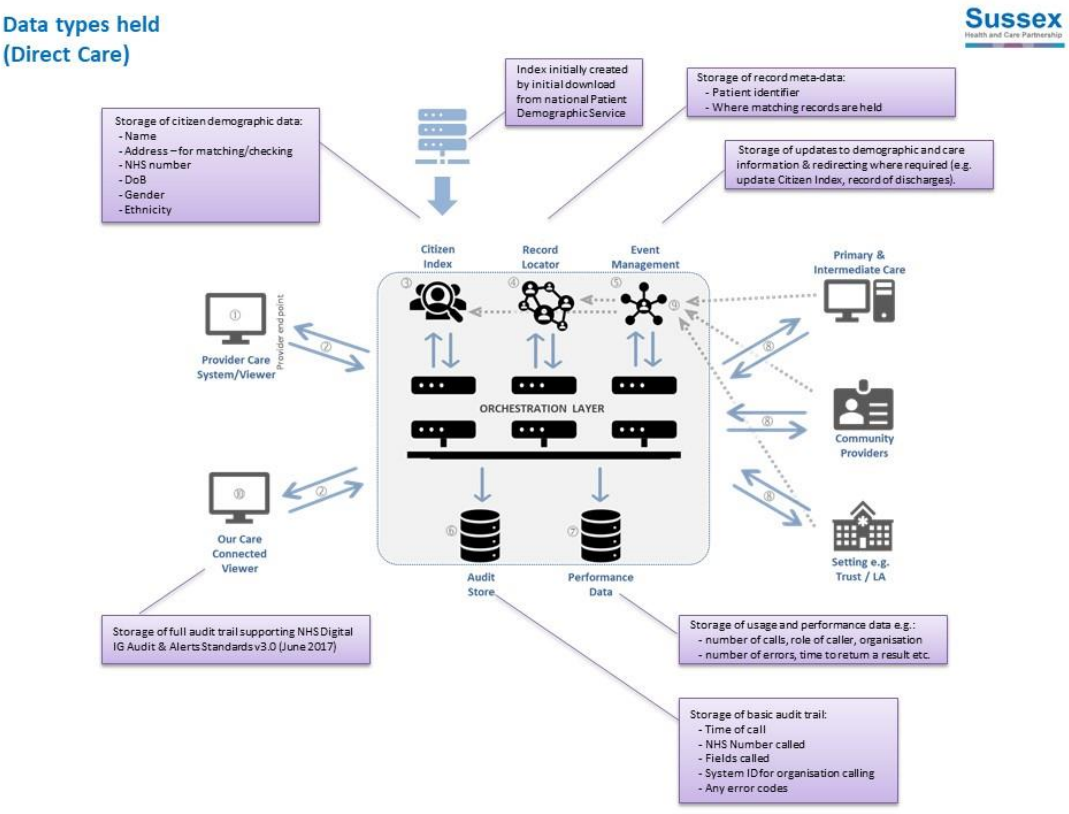
11 **Has a data flow mapping exercise been undertaken?**

The approach is a technical solution, called the "Orchestration Layer" which enables care providers to exchange data needed for Direct Care.



NO	FUNCTION	SECURITY
①	Practitioner access and display of aggregated view	Must log in via role-based access secure portal, in-context call trigger, with audit log.
②	"Call" message & "view" return to/from Orchestration layer end point.	Only NHS number sent, over secure (e.g. https) link
③	Holds demographic data for all citizens to check consistency and provide reliable identifier for Orch. Layer.	(e.g. some patient may not have NHS no)
④	Holds note of all health/care records for citizens, and in which system they are held	
⑤	Gets feed from all systems on events (e.g. discharges, demographic updates etc.), adds to view & updates ⑤ & ④	

NO	FUNCTION	SECURITY
⑥	Logs clinical interactions with system for audit assurance/investigation	Limited to NHS number, system called, fields retrieved (not content), time
⑦	Holds activity-type data for monitoring usage and performance, diagnostics	
⑧	"Call" to clinical systems & return data	Two-way secure link e.g. https or via GP Connect
⑨	Update messaging to Event Management from across ICS	Sent via secure link e.g. https, HL7 messaging
⑩	OCC Viewer – enables access where provider unable to display from end-point	Holds user authentication and full audit. Access using secure password.
	Orchestration Layer	On secure Microsoft Azure tenancy held by ESHT



	Providers will agree the specific datasets and technical configuration as part of the onboarding process or as part of a change process to ensure the safeguarding of patient and service user information in line with the Technical Standards as set out by the SCHP Infrastructure Standards Group. Information provided will be in line with standards as set out by the Professional Records Standards Body (PRBS). The Citizens Index will hold Demographic Information and as part of the development of this component part, a separate DPIA and technical assessment will be completed. Any additional developments to the Sussex Shared Care Record will receive further data protection, clinical and Technical assessments.
12	**What is the source of the data?** The source of the data will be from Sussex Health and Care Partnership Providers. All of the data will be integrated digitally using Application Programming Interface (APIs) between the line of business systems and the Orchestration Layer (Integration Engine). The Citizen's Index will utilise demographic data from the National Patient Demographic Service.
13	**Where will the data be stored (physical or electronic location):** The Sussex Shared Care Record operates within a secure Microsoft Azure Environment. The Orchestration Layer does not hold data. Data only flows through the Orchestration Layer. Information will remain within each organisation's on Health Care Record System and will be made available to view (on request*) across Health and Care Practitioners within the Sussex Health and Care Partnership. Partners within SHCP are detailed within Information Sharing Gateway Reference: DS004770 and DF007001. Information within the Citizens Index, the Record Locator Service and the Event Management will be 'held' by East Sussex Healthcare Trust as the host Data Processing organisation under contract.
14	**Who will have access to the data?** • Health and Care Practitioners within the Sussex Health and Care Partnership (signed up through the ISG) with a legitimate relationship to the patient or service user, will be able to view information which is flowed through the Sussex Shared Care Record. The viewing systems will all have secure, role-based access protocols with audit trails. • Sussex Shared Record System Administrators within East Sussex Healthcare NHS Trust will have access to the secure Azure environment and access will be via secure access controls.
15	**Will you be sharing data with anyone?** Information will remain within each organisation's on Health Care Record System and will be made available to view (on request*) across Health and Care Practitioners within the Sussex Health and Care Partnership. Partners within SHCP are detailed within Information Sharing Gateway. *information is 'called' and viewed from within an organisations health and care system or viewing portal. The Sussex Shared Care Record is designed to enable the 'sharing' of data to support

	improvements in the safety and quality of care. Information within the Citizens Index, the Record Locator Service and the Event Management will be 'held' by East Sussex Healthcare Trust as the host Data Processing organisation under contract.
16	**Is there an ability to audit access to the data?** Yes. Part of the technical design includes audit processes.
17	**Does this activity propose to use data that may be subject to or require approval from NHS Digital?** Yes, for example access to data via GP Connect and the National Patient Demographic Service will require approval from NHS Digital.
18	**What is the current state of technology in this area?** There are numerous programmes seeking to achieve the same end-result around the country. Part of the national programme function is to determine the benefits and disadvantages of the various approaches. Cloud technology and system integration is now in a mature state and the technical background has evolved such that Internet/Cloud First is now a National Policy and all public sector organisations are required to consider this as a solution before looking at alternatives. https://digital.nhs.uk/services/internet-first/policy
19	**Is there an approved Technical Assessment process in place for any system(s) processing data:** The Sussex Health and Care Partnership has an Infrastructure Standards Group as part of its governance structure. The group comprises technical experts and digital leads from across Sussex who review, assess and oversee the technical security, functionality and resilience of systems adopted or developed within the Our Care Connected programme This group approves the technical standards which support the development of the Our Care Connected Platform. All new and changes to development will be assessed and assured against agreed standards and any divergence from standards will be reviewed and signed off.
20	**Are you proposing to use a third party/processor/system supplier as part of this project/activity?** Yes 1) East Sussex Healthcare NHS Trust (ESHT) 2) Microsoft Azure (tenancy held by ESHT)
	Has the third party met the necessary requirements under the GDPR and Data Protection Act, and a contract in place? **1) East Sussex Healthcare NHS Trust** • Data Processing Contract in place • Compliant to the Data Security and Protection Toolkit **2) Microsoft Azure (tenancy held by ESHT)** • Microsoft Azure operate under a standard contract with ESHT and included within the Associated Documents Section within the Information Sharing Gateway Reference:

	DF007001
	Are there any ICO enforcement, decision notices, audit or advisory visit against the organisation? No
21	**Are you transferring any data outside of the UK?** No
22	**What security and audit measures have been implemented to secure access to and limit use of personal identifiable information?** Information will remain within each organisations on Health Care Record System and will be made available to view (on request*) across Health and Care Practitioners within the Sussex Health and Care Partnership. Partners within SHCP are detailed within Information Sharing Gateway. Access wil be subject to the data security controls assigned to the system and aligned to Role Based Access Controls. *information is 'called' and viewed from within an organisations health and care system or viewing portal. Organisations surfacing/viewing information must be compliant to the NHS Digital Data Protection and Security Toolkit, or similar standards, and maintained on an annual basis. Access to the Data Architechture will be under strict policy and access controls and assessed by the Sussex Health and Care Partnership Infrastructure Standards Group. Information within the Citizens Index, the Record Locator Service and the Event Management will be 'held' by East Sussex Healthcare Trust as the host Data Processing organisation under contract. The technical design of the Sussex Shared Care Record includes robust audit processes managed through the Infrastructure Standards Group.
23	**Is Mandatory Staff Training in place for the following; Data Collection; Use of the System or Service; Collecting Consent (common law); Information Governance?** All parties to the Information Sharing Agreement must be compliant to the NHS Digital Data Protection and Security Toolkit, or similar standards, and maintained on an annual basis.
24	**Will the process ensure the quality of the data being processed?** Yes, demographics processed will be checked against the National PDS and will update the citizens index. Data quality will be included as part of technical design and signed off by the TDA.
25	**What assurances are in place for the decommissioning of any IT systems or medical devices? (IT systems & medical devices only)** Contractual. Any decommissioning of systems will be managed through robust project management which will includes what happens to the data.
26	**What is the nature of your relationship with the individuals?** Health and Care Patients, Service Users and carers.
27	**How much control will individuals have over their processing?** Sharing information through the Sussex Shared Care Record is for direct care purposes.

	Type 1 opt-outs (sharing for indirect or secondary purposes) are not applicable to this sharing. Where a patient or service user dissents to share information with other providers within Sussex (sets a record to not share) this is recorded in the provider system and will not be surfaced into the Sussex Shared Care Record. The Sussex Shared Care Record processing will respect any such consent options and described in the associated Technical Specification. Information processed via GP connect, withholds any data with opt-out recorded.
28	**Would they expect you to use their data in this way?** The Our Care Connected programme aims to engage patients, service users, providers and stakeholders to communicate its general purposes. The To Share or not to Share Government Response to the Caldicott Review, (Department of Health, 2013) reports: *For the purposes of direct care, relevant personal confidential data should be shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual.* *Most people would expect and want this to happen routinely, but would also want assurance that only those involved in their care should have access to confidential information, unless they have given specific consent for other purposes.* Strict access controls and audit processes will be in place to ensure only health and care practitioners who have a legitimate relationship with a patient or service user (e.g. is registered or referred into their care). Staff are contractually and professionally bound by the GDPR (Article 5) and Caldicott Principles in regard to use and access of information.
29	**Do they include children or other vulnerable groups?** Yes
30	**Are you aware of any existing concerns over the use of the data?** No
31	**What types of processing identified as likely high risk are involved?** The processing will include special categories of information as defined in the General Data Protection Regulation / Data Protection Act. However, information will be appropriate (in line with the Professional Records Standards Body, and only shared with health and care practitioners involved in a patient / service user's care.
Individuals Rights	
32	**Will patients be asked for consent (common law) for their information to be collected and/or shared?** Sharing is based on implied consent. Provider organisations are responsible for informing patients and service users on the processes for collection and uses of their data and should be included within their own privacy notices. A template privacy notice will be available to organisations.
33	**What changes are proposed to Fair Processing Notices of the organisations involved (Privacy Notices)?** Organisations will need to ensure their privacy notices are updated to include the use of their

	data for the Sussex Shared Care Record. A template privacy notice will be available to organisations. Information will be available also on the Sussex Health and Care Partnership Website.
34	**National Data Opt-Out** N/A processing is only for direct care.
35	**Please set out the process for responding to requests under the right of access by data subjects.** Data for the Sussex Shared Care Record is held within each provider's own health care record systems. Therefore each organisation is a data controller in their own right and are responsible for their own subject access requests (with support where required from the Our Care Connected Technical Host or Information Governance Lead). Access to information held within the Citizens Index will follow the Host Organisations Subject Access processes in conjunction with the joint data controllers and will be detailed in the Citizens Index DPIA.
36	**Please detail how this data will be made portable if requested by the data subject.** Data for the Sussex Shared Care Record is held within each provider's own health care record systems. Therefore each organisation is a data controller in their own right and are responsible for manging requests (with support where required from the Our Care Connected Technical Host or Information Governance Lead).
37	**Please detail how data subjects will be able to request the erasure/rectification of the data being processed. (Please see guidance for details on when this right is available).** Data for the Sussex Shared Care Record is held within each provider's own health care record systems. Therefore each organisation is a data controller in their own right and are responsible for responding to requests. The Right to Erasure does not apply in this case as that processing is necessary for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (GDPR Article 17(3)(b)).
38	**How long is the data/information to be retained?** Data for the Sussex Shared Care Record is held within each provider's own health care record systems. Therefore, each organisation is a data controller in their own right and are responsible for the retention of information in accordance with the Records Management Code of Practice for Health and Social Care.
39	**How will it be possible to restrict the processing of personal data about a particular individual should this become necessary?** Patients or service users may dissent to sharing information with other health and care providers. This should be discussed with the health care practitioner providing care to

	ensure there is no impact on their care. The Sussex Shared Care Record processing will respect any such opt-out options and will be assessed and assured as part of the Technical Specifications. Individuals with sensitivity flags or other legal restrictions will not be processed through the technical architecture of the Sussex Shared Care Record, therefore will not be available to recipient systems.
40	**If the organisation/service ceases what will happen to the data?** Information is held by each organisation as Data Controllers and any data will be managed in accordance to the Records Management Code of Practice for Health and Social Care (Information Governance Alliance, 2016). Should the host organisation cease, this will be managed under robust programme and information governance management.
41	**What plans are in place in relation to the internal reporting of a personal data breach?** Information breaches will be regarded as serious and result in an investigation which may include disciplinary action. 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. Organisations will agree an approach regarding onward reporting and investigation, supported by the Sussex Shared Care Record Host and the Sussex Health and Care Partnership Information Governance Steering Group.
42	**What plans are in place in relation to the notification of data subjects should there be a personal data breach?** 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. 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. Organisations will agree an approach regarding onward reporting and investigation, supported by the Sussex Shared Care Record Host and the Sussex Health and Care Partnership Information Governance Steering Group.
43	**Will any personal data be processed for direct marketing purposes? If yes please detail.** No
44	**Will the processing result in a decision being made about the data subject solely on the basis of automated processing (including profiling)?** No
Risks, issues and activities	
45	**What is the impact if the project/process does not go ahead?:** Our Care Connected is a directive under the NHS Long Term Plan.

	Not proceeding will impact the crucial opportunity for improved care from having the right information available at the right time, and to the right practitioner. A shared care record across care systems is a priority within the third phase of NHS response to COVID-19, to be delivered by September 2021, allowing the safe flow of patient and service user data between care settings.
46	**How will you prevent function creep?** There will be robust governance processes in place through the Sussex Health and Care Partnership Governance structures. Any changes to data processing will be agreed through a formalised agreement and reviewed through the Sussex Health and Care Partnership Information Governance Steering Group and where required, a new DPIA completed.
47	**Have any Information Governance risks been identified relating to this project?** Yes
48	**Is an Information Sharing Agreement required?** Yes
49	**Any further comments to accompany this DPIA that should be considered?** **Data Controller Statement** The providers of information as stated within the Information Sharing Gateway will be considered as Joint Data Controllers. 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." Information is made available via each organisation's health care record system or via a dedicated portal (where an organisation's system does not support full system integration. Each organisation will: • Comply with its obligations under General Data Protection Regulation 2016; Data Protection Act 2018; Freedom of Information Act 2000; and Environmental Information Regulations 2004 and other legal requirements (see Appendix B) • Use the information shared solely for the purposes identified and shall not process the information for any other purposes. • Ensure that information is accurate, complete and up to date. • Treat the information as confidential and safeguard it accordingly. Respect for the privacy of individuals will be afforded at all times. • Ensure that they are properly registered under Data Protection laws and to ensure that policies and procedures are in place to comply with their statutory responsibilities. • Ensure they are compliant to the NHS Data Security and Protection Toolkit or similar assurance framework. • Ensure compliance with any specific legal requirements regarding the disclosure of

	information. • Take responsibility for putting in place systems, issuing specific guidance and for providing training to their staff to ensure compliance with this agreement. • Take appropriate measures to ensure that security arrangements are in place to prevent unauthorised access to and disclosure of personal information and will be open to scrutiny by other organisations to this agreement upon request. • Nominate a designated person who will assume responsibility for the operation of this agreement and for the requesting and disclosure of information, security and confidentiality. • Disclosures and requests for disclosures must be recorded and retained by each organisation. **Common Law Duty of Confidentiality** Each organisation is responsible for ensuring that where information is shared on the basis of implied consent the following conditions are met: • The Information is shared in order to provide and support the direct care of the patient or service user. • Explanatory information is readily available to patients and service users on how their information is be used; who this will be shared with/viewed by; the legal basis for sharing; and their right to object. This can be provided in leaflets, posters, on websites, and face to face. It should be tailored to patients and service user's identified communication requirements. • There is no reason to believe they have objected. • Assurance is in place that anyone information is shared with/viewed by understands that this is being shared in confidence and for the purpose of providing and supporting the direct care of the patient or service user. The governance of the Sussex Shared Care Record will be via the Sussex Health and Care Partnership Digital Programme Board and its relevant sub-groups, including the Information Steering Group, in consultation with the Data Controllers.

Data Protection Impact Assessment - Part 3

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

Sussex Health and Care Partnership

Probability (P)	Impact (I)				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
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 PxI=R	Controls	Actions	Is the Risk at an accepted level?*
1	Processing is unlawful / Unfair	2 x 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, including Role/Position Based Access Controls. Data Processor Contract in place.	Information sharing agreements to be signed off in ISG. Privacy Notices Template for programme Providers to ensure own Privacy Notices are in place.	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, including Role/Position Based Access Controls	Information sharing agreement Privacy Notices for programme	Yes
3	Personal data is not held securely and an incident occurs	1 x 4 = 4	DSPT compliance by all parties (including data processor) Information security controls in place, including Role/Position Based Access Controls. Existing fair processing and privacy notices Data Processor Contract in place	Technical Assessment completed and approved at Sussex Health and Care Partnership Infrastructure Standards Group	Yes
4	Breach of confidentiality – unlawful access to record (by staff / external parties)	1 x 4 = 4	DSPT compliance by all parties (including data processor) Information security controls in place, including Role/Position Based Access Controls. Existing fair processing and privacy notices Data Processor Contract in place	Technical Assessment completed and approved at Sussex Health and Care Partnership Infrastructure Standards Group. Information sharing agreements to be signed off in ISG.	Yes
5	Loss or alteration of data (temporary or permanent), due to technical / security failure	1 x 4 = 4	DSPT compliance by all parties (including data processor) Information security controls in place, including Role/Position Based Access Controls.	Technical Assessment completed and approved at Sussex Health and Care Partnership Infrastructure Standards Group.	Yes
6	Poor quality data impacting on quality of care delivery	1 x 4 = 4	All organisation have a responsibility for data quality, ensuring datasets are reporting	Ensuring robust guidance and standards are provided to providers to ensure data	Yes

			accurately.	processed is appropriate.	
7	Excessive processing of data.	1 x 4 = 4	Governance Structures.	Ensuring change control processes are in place.	Yes
8	Partners failing their compliance requirement (e.g. DSPT/ICO Notification)	1 x 3 = 4	Contracting requirements Monitoring via SHCP Information Governance Steering Group Information Sharing Gateway Assurance Statements.	Reviews through SHCP Information Governance Steering Group.	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.
Demographics	Details such as name, address, date of birth and NHS Number.
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 or service users 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 / service user's clinical record.
Information Sharing Gateway (ISG)	The ISG is an administration portal to manage information sharing agreements and data flows and the approval and signatory process. The ISG assists an organisation's compliance with the General Data Protection Regulations (GDPR) and their responsibilities under the Data Protection Act; helping to ensure information is being shared, managed and processed correctly. It centralises and shares key resources in a way that is accessible and transparent. www.informationsharinggateway.org.uk
legitimate relationship	The care relationship between a patient/service user and a healthcare practitioner or group of healthcare practitioner. It ensures that only care practitioners involved in the patient/service user care can access the clinical information.
Joint Data Controller	Two or more parties acting together to decide the purpose and manner of any processing**.**
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 and Data Protection Act.

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