NHS
Somerset
NHS Foundation Trust

DPIA01 FORM: *DATA PROTECTION AND PRIVACY IMPACT SCREENING*

The following screening questions will help our team decide whether a full data protection and privacy assessment is necessary. Your answers will provide an indication whether a full assessment must be undertaken.

Q1	The details of responsible lead to the project	Name	[redacted]
		Title	**SIDeR Programme Manager**
		Department	**Somerset CCG**
		Telephone	[redacted]
		E-mail	[redacted]
Q2	The details of the Information Asset Owner	Name	[redacted]
		Title	**Chief Operating Officer**
		Department	**Somerset CCG**
		Telephone	
		E-mail	
Q3	The name of the project	**Somerset Integrated Digital Electronic Record (SIDeR)**	
Q4	Reference to project or scheme reference number		
Q5	Estimated completion date of project:	**March 2021**	
Q6	Describe the project background, why has the project been initiated?	Everything that we do must contribute to the following strategic objectives:- • Records largely paperless by 2020 • Records accessible to Health and Social Care • Records accessible in real time • People able to view and annotate their health record online	
Q7	Describe in a few sentences the benefits, quality expectations and intended outcomes:	The focus of this Programme is to improve direct care for people through enabling care information to be shared electronically. Other examples of key SIDeR objectives include: • Reducing the need for the people to continually have to repeat their story; • Reducing delays to treatment due to insufficient information; • Improving safety; • Providing information in electronic form; • Contributing to the paper free agenda; • Providing services to enable people to view and in the longer term, contribute to their own care record	

Q8	Describe the constraints to the project:		The primary objective of this Programme is to share information within the NHS and between the NHS and Social Care, to improve direct care. Given the existing breadth of this Programme of work, it is important to limit the scope to connecting the systems listed on page 10 as well as the key deliverables and services listed in 3.7 above. (NB references are to the SIDeR PID v1.0)
Q9	Does the project include any of the following activities;	**Y**	Retrieval, obtaining, recording or holding information or data
		Y	Alignment, matching, combining, organisation, adaptation or alteration of information or data
		Y	Consultation or use of information or data
		N	Blocking, erasure or destruction of information or data
	Q9 not applicable	**Y**	Disclosure or sharing of information or data
Q10	Do the project activities include any of the following data sets;	**Y**	**Personal identifiable details** (e.g. name, address, e-mail address, postcode, date of birth)
		Y	**Identifier numbers** (e.g. NHS, national insurance, passport, driving license numbers)
		N	**Genetic data** (e.g. DNA, an individual's gene sequence)
		N	**Biometric data** (e.g. fingerprints, facial recognition, retinal scans)
		Y	**Family, lifestyle and social circumstances** (e.g. marital status, housing, travel, leisure activities, membership of charities)
		Y	**Vulnerable individuals** (e.g. refer to safeguarding policies)
		N	**Education and training details** (e.g. qualifications or certifications, training records)
		N	**Employment details** (e.g. career history, recruitment and termination details, attendance details, appraisals)
		N	**Financial details** (e.g. banking, income, salary, assets, investments, payments)
		N	**Goods or services** (e.g. contracts, licenses, agreements)
		Y	**Legal details** (Treatment Escalation Plans, NOK details)
		Y	**Cultural identity including racial or ethnic origin**
		N	**Political opinions, religious or philosophical beliefs**
		Y	**Health data** (e.g. treatment, diagnosis, medical information including a physical or mental health or condition)
		N	**Location data** (e.g. GPS location, Wi-Fi tracking, vehicle tracking)
		N	**Technology identifiers** (e.g. device names, applications, tools, protocols, such as IP addresses, cookie identifiers, radio frequency identification tags)

		N	**Criminal proceedings** (e.g. convictions, outcomes, sentences including offences or alleged offences)
	Q10 not applicable	**N**	**Sexual life** (e.g. sexual health, sex life or sexual orientation)

Q11	Does the project include any of the following activities;	Y	**Evaluation or scoring, including profiling** (e.g. credit scoring, fraud protection, questionnaire's that generate a profile to an individual) EFI – frailty scoring
		N	**Automated decision-making** (where a decision is taken without human intervention e.g. automated system, algorithms)
		N	**Direct marketing** (e.g. newsletters, postcards, telemarking, e-mail subscriptions)
		N	**Systematic monitoring of individuals** (e.g. CCTV, body camera's, health data through wearable devices)
		N	**Storing or transferring data outside the EU** (e.g. cloud computing, accessing data outside the EU, use of an American transcribe company)
		Y	**Processing data on a larger scale** (more than 11 individuals)
		N	**Characteristic's which may affect an individual's legal rights or responsibilities ultimately preventing the exercise their rights or contract**
		Y	**Implementation** of a new technology, system or business process or collection of new information
		Y	**Change** to existing technology, system or business process will significantly amend the way in which data or business is handled or used
	Q11 not applicable	Y	**Use of a supplier**

END OF DPIA01

DECLARATION

This DPIA01 form and declaration **must** be completed and approved by the IG Working Group.

Responsible project lead	[redacted]
Project name	**SIDeR**
Project or scheme reference number	
Estimated project completion date	**March 2021**

Some of the screening questions within this document apply to the above project; therefore, it is likely that a full Data Protection and Privacy Impact Assessment must be undertaken. I understand that at this stage the Data Protection Officer must be involved and the outcomes must be integrated into the project plan before the project is developed and implemented.

Signed:	[redacted] **(Programme Manager) – Head of Digital Transformation**
Dated:	**June 2019**

DPIA02 FORM: *SUPPLIER OVERVIEW*

S1	What is the name of the supplier company?	Black Pear NB their DPIA is available at: https://support.blackpear.com/hc/en-us/articles/360021963871-Data-Privacy-Impact-Assessment	
S2	Is this supplier a subsidiary company? If so enter the name of the parent company.	Contract is held by Soft Cat. Black Pear are a sub contractor to them. Black Pear is a wholly owned private limited company	
S3	Does the parent company have the power/hold the subsidiary company accountable for its performance?		**Yes** *the remaining questions must be completed for the parent company*
			No *the remaining questions must be completed subsidiary company*
S4	What is the company's registered address?	Bartlam House Shrawley Worcester WR6 6TP	
S5	Is the company data protection registered with a supervisory authority such as the ICO? If so please provide details of the registration:	**Supervisory Authority Name:**	Information Commissioner's Office
		Registration Number:	ZA215442
S6	Has the company appointed a data protection officer? If so please provide the DPO contact details:	[redacted]	
S7	Has the company attained any certifications, seals or marks to demonstrate compliance with data protection law? If so please provide details:	ISO27001 (for AWS – 2013-009)	
S8	Are the company's employees trained in confidentiality? If so please provide details:	Black Pear is IG Toolkit accredited as provided in procurement. All employees receive Information Security training using recognised on line training services and certification. In line with our IG Toolkit and GPSOC Lot1 obligations, employees must renew their certification and training at least annually unless there is any changes in between regarding policy, legislation etc that requires more immediate updates. Whenever our information security policy changes all employees are advised and asked to review and confirm understanding and compliance in writing.	
S9	Is the company registered and compliant with the Department of Health's Data Security and Protection Toolkit (formally known as the IG Toolkit)? if so please provide details of the registration:	**Registration Number:**	ODS code: 8HV05
		Score:	Standards Met 15/03/1
S10	Has the company attained any of the listed standards:		**ISO27001**: *Information Security Management, if so please obtain a copy of the certification (Obtained for AWS)*
			ISO29100: *Privacy Framework Standard, if so please obtain a copy of the certification*

			Cyber Essentials (CE) or Plus (CE+) certification				
			UK Digital Marketplace				
			PCI DSS: *Only applicable to card payment activities*				
		X	**Cloud Computing Standards:** *Only applicable to remote server developments*				
S11	Does the main contract include Data Protection and Freedom of Information provisions?	**X**	**Yes**	**Contract review undertaken as part of regular contract review schedule (Oct 19)**		**No**	

DPIA02 FORM: *SUPPLIER OVERVIEW*

S1	What is the name of the supplier company?	NHS South, Central and West Commissioning Support Unit (part of The NHS Commissioning Board 'NHS England')		
S2	Is this supplier a subsidiary company? If so enter the name of the parent company.	Sub-contract is with Black Pear whose contract is held by Soft Cat. Black Pear are a sub contractor to them. Black Pear is a wholly owned private limited company		
S3	Does the parent company have the power/hold the subsidiary company accountable for its performance?		**Yes**	*the remaining questions must be completed for the parent company*
		X	**No**	*the remaining questions must be completed subsidiary company*
S4	What is the company's registered address?	The NHS Commissioning Board (NHS England) Quarry House Quarry Hill Leeds LS2 7UE		
S5	Is the company data protection registered with a supervisory authority such as the ICO? If so please provide details of the registration:	**Supervisory Authority Name:**	Information Commissioner's Office	
		Registration Number:	Z2950066	
S6	Has the company appointed a data protection officer? If so please provide the DPO contact details:	[redacted]		
S7	Has the company attained any certifications, seals or marks to demonstrate compliance with data protection law? If so please provide details:	Cyber Essentials Plus (issued 11/09/2019)		
S8	Are the company's employees trained in confidentiality? If so please provide details:	All employees receive Information Security training using recognised on line training services and certification. In line with the Data Security and Protection Toolkit, employees must renew their certification and training at least annually unless there is any changes in between regarding policy, legislation etc that requires more immediate updates.		
S9	Is the company registered and compliant with the Department of Health's Data Security and Protection Toolkit (formally known as the IG Toolkit)? if so please provide details of the registration:	**Registration Number:**	ODS code: 0DF	
		Score:	Standards Exceeded 31/03/2020	
S10	Has the company attained any of the listed standards:		**ISO27001**: *Information Security Management, if so please obtain a copy of the certification*	
			ISO29100: *Privacy Framework Standard, if so please obtain a copy of the certification*	
		✓	**Cyber Essentials (CE) or Plus (CE+) certification**	
			UK Digital Marketplace	
			PCI DSS: *Only applicable to card payment activities*	
			Cloud Computing Standards: *Only applicable to remote server developments*	

S11	Does the main contract include Data Protection and Freedom of Information provisions?	✓	**Yes**	**Contract review undertaken as part of regular contract review schedule (Oct 19)**		**No**

DPIA03 FORM: *LAWFULNESS OF PROCESSING*

L1	The information processed about: Also known as data subjects, individuals and natural persons		**Employees**
		X	**Patients**
			Students
			Business partners or organisations
			Other
L2	The sources of information are:	X	**Obtained from the individual directly**
		X	**Obtained indirectly from another source**
			Publicly available
			Other
L3	For the processing of personal data to be lawful, you need to identify a lawful basis:		**6(1)(a)** Consent of the data subject.
			6(1)(b) Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract.
		Y	**6(1)(c)** Processing is necessary for compliance with a legal obligation.
		Y	**6(1)(d)** Processing is necessary to protect the vital interests of a data subject or another person.
		Y	**6(1)(e)** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
			6(1)(f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data in particular where the data subject is a child.
L4	For the processing of special categories of data to be lawful, you need to identify a lawful basis:		**9(2)(a)** Explicit consent of the data subject.
		Y	**9(2)(b)** Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement.
		Y	**9(2)(c)** Processing is necessary to protect the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent.
			9(2)(d) Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
			9(2)(e) Processing relates to personal data manifestly made public by the data subject.

			9(2)(f) Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
		Y	**9(2)(g)** Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
		Y	**9(2)(h)** Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
		Y	**9(2)(i)** Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
			9(2)(j) Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

If you are relying on consent, please complete: (NB SIDeR does not rely on consent, but some of the items below are still relevant, so have been completed)

L5	Consent requires a positive action by the individual, rather than being assumed as the default.		**Consent N/A**
L6	Consent is obtained through:		**Consent N/A**
L7	Consent is recorded:		**Consent N/A**
L8	If so, how will the consent be collected and recorded?		**Consent is not the basis for the processing of data on SIDeR**
L9	Can the individuals withdraw or opt-out from their data being processed?	Y	**Yes – Individuals can exercise their GDPR article 21 rights to object. That is not a 'free choice' opt out. The DSA outlines how this is managed. The individual can raise an objection if they are with the care professional at the point of access and that can be managed directly.** **If an individual has an objection at another time (i.e. to the principle rather than a specific time of use) then they must raise that with the organisation(s) who they have concerns about data sharing with. Those organisations will discuss the concerns and aim to agree an appropriate response, balancing the concern of the individual and the need of the system to share data for effective care delivery**

L10	How will the withdrawal or opt-out be managed and recorded?		**If there is an objection related to data being shared by a specific partner (or partners) to SIDeR, then each partner will respond and record the outcome of discussions with the individual.** **If there is an objection in general to the use of SIDeR, then as the data does not reside in a repository and is only called from systems when it is needed, then that will be dealt with by the organisation the individual is raising concerns with at the time. SIDeR does not feature a method to record this, but individual organisations can note in their own record systems**
L11	Notice was provided to the individuals prior to collection of data?	Y	**Your Somerset newsletter – Dec 17, April 18 – Sept 18 & Dec 18 and others feature sharing articles highlighting SIDeR. EMIS viewer documents adapted for GPs and new Fair Processing Notices promoted. Common messages developed for integration with partner fair processing notices. This is a regular review item for the IG working group**
			No
L12	The data will be used for the following purposes:		**Initial purposes are all related to the sharing of data to provide effective care services across partner agencies. This is where the organisations already have the legal gateways to share and where an electronic method of sharing will be more effective, more timely and more complete than letters, emails, calls etc.**
L13	Do you envisage using the information for any other purpose in the future? If so, provide details:		**It will in time be developed to support analytical activities, related both to managing and planning services, and also improved prevention and interventions, where analysed data will 'case find' individuals who can be approached for different care delivery models coming where possible from a preventative angle.**

L14	When the data is collected, the individual is informed: See L11 also note - Some elements 'use case' specific'				
	All the purposes of processing		**Yes**		**No**
	The categories of data processed		**Yes**		**No**
	The individuals freedoms and rights		**Yes**		**No**
	If the information is shared and with whom		**Yes**		**No**
	If third party access is envisaged		**Yes**		**No**
	Our data protection responsibilities		**Yes**		**No**
	Our identity as a data controller		**Yes**		**No**
	Our data protection supervisory authority		**Yes**		**No**
	Our obligation to respond to questions		**Yes**		**No**
	Consequences for un-lawful processing or data breaches		**Yes**		**No**
L15	When the data is not collected, but used the individual is informed: - **SIDeR users will be encouraged to inform the individual that they can access the record at the point of care delivery and will deal with any concerns raised at that time. The full list of items below won't necessarily be informed in a face to face (or on phone) setting**.				

	All the purposes of processing		**Yes**		**No**
	The categories of data processed		**Yes**		**No**
	The individuals freedoms and rights		**Yes**		**No**
	If the information is shared and with whom		**Yes**		**No**
	If third party access is envisaged		**Yes**		**No**
	Our data protection responsibilities		**Yes**		**No**
	Our identity as a data controller		**Yes**		**No**
	Our data protection supervisory authority		**Yes**		**No**
	Our obligation to respond to questions		**Yes**		**No**
	Consequences for un-lawful processing or data breaches		**Yes**		**No**

DPIA04 FORM: *DATA QUALITY*

D1	Who will be able to access the data? Include internal users, third parties, business partners etc.	Each 'use case' will determine the specific users for each SIDeR related activity. In the first instances all uses will be health and care provision related and data will be available to appropriate staff in the partner organisations involved in service provision
D2	Who will record or input the data? Include internal users, third parties, business partners etc.	Each 'use case' will also determine this specifically, but in general terms, data will either be sourced from existing systems or both extracted and added to (i.e. End of Life Records)
D3	Who will be able to amend the data? Include internal users, third parties, business partners etc.	**Each use case will determine this specifically, again based on the 'need to know/need to use' principles**
D4	What training will the users receive for accessing, inputting or amending the information or data?	Specific for some services / use cases plus general training on the overall SIDeR service
D5	Will the information or data be checked for accuracy?	X **Yes** **No**

D6	Have you defined a standard operating procedure covering the following activities? (the indication is 'will be')				
	Revoking and approving user access to the data	**X**	**Yes**		**No**
	Developing and maintaining staff competences for record keeping and data quality		**Yes**	**X**	**No**
	Ensuring timely, accurate and complete recording of data	**X**	**Yes (for use cases recording data)**		**No**
	Addressing and escalating data quality issues in a timely manner	**X**	**Yes**		**No**
	Consideration of compliance with legislation and local procedures	**X**	**Yes**		**No**
	Ensuring all data is handled in a secure and confidential way	**X**	**Yes**		**No**

	Correcting or merging data inaccuracies	**X**	**Yes**		**No**
	The erasure, blocking of data	**X**	**Yes**		**No**

D7	Describe the steps which shall be taken to ensure that the information is accurate, complete and up-to-date:	**Data extracted from source systems will be dependent on the quality of data within those systems. Surfacing the data in a shared environment tends to lead to identification of possible inaccuracies and the governance framework and education will ensure staff are aware to report (to partner staff if required) any inaccuracies identified.** **During the testing phase, the quality of data and the presentation will be assessed using records taken from core supporting systems where the record relates to a deceased individual. The identity will be replaced with a false identity so that it is neither a real live person, nor the identifiable record of a deceased individual, but the data is as close to 'real' it can be rather than made up example patients. This approach has been discussed at the technical working group, the IG working group and the Digital Delivery Board for sign off before being undertaken**

DPIA05 FORM: *ON-GOING USE OF DATA*

O1	What checks have been made regarding the adequacy, relevance and necessity of data used?	**Each 'use case' will determine the relevant data to be shared for that activity. This will be on the basis of 'building up' the dataset from scratch, so that clear need for each item of data is identified.**				
O2	Which format will the data be stored in?	X	**Electronic**			
			Paper			
			Other			
O3	Where will the data be stored?	**Amazon Web Services data centres within England (AWS EU London Region)**				
O4	Will there be any data stored in a country outside the European Economic Area?		**Yes**	**X**	**No**	
O5	Will the project activities include data which was not previously collected?	X	**Yes**		**No**	
O6	Will the project activities make data more readily accessible than before?	X	**Yes**		**No**	
O7	What training have users had in confidentiality?	**All users will have undertaken mandatory IG training as part of their organisational compliance with IG toolkit/Data Security & Protection toolkit.**				
O8	Have you assessed the likelihood of the use of the data causing unwarranted distress, harm or damage to data subjects concerned?	**Each 'use case' will have to address this specifically, but the overall intent is to use data to improve the provision of care directly to individuals, so in general the likelihood of harm is very low, and in truth the opposite should be achieved. However informing activities will give individuals opportunity to raise concerns and potentially utilise their right to object.**				
O9	Have you assessed the likelihood of the loss or damage of the data causing distress, harm or damage to data subjects concerned?	**The data used is health and care data, therefore any loss or damage to this data has the potential to distress or harm the data subject. Therefore stringent security controls will be applied (Defined in DPIA 06 technical and security measures)**				
O10	Could the project activities result in making decisions and or taking action against the individuals in ways that could have significant impact on them?	**The results will in virtually all cases benefit the data subject. The decisions will not be made by automated means**				
O11	Could the project activities interfere with the privacy under article 8 of the Human Rights Act?	**As health and care data is considered private and confidential then there is the potential, but the sharing of data will generally be done with the knowledge of the individual and the opportunity for them to object (Use cases will define any specifics around this)**				

O12	What is the data retention period for this data? (The retention schedules set out in the Records Management NHS Code of Practice.)	**Data extracted from other systems will be subject to the retention period for the source system. Any use case where data is specifically recorded will detail the retention period based on NHS and Local Authority guidance**
O13	Where will the data be archived?	**Amazon Web Services data centres within England (AWS EU London Region) will hold the data during active use. When the minimum retention periods for any data that persists (i.e. EPACCS) have been reached, then this will be reviewed as to whether there is a need to retain the data. Retention periods will be from the NHS Records Management guidance and any appropriate Local Government Association guidance. This is likely to be a minimum of at least 8 years.**
O14	How will the data be destroyed when it is no longer required?	**On termination of service, Black Pear will transfer the data to the data controller(s) via strongly encrypted media and secure transport. Not more than 30 days after the data will be deleted from the service infrastructure. AWS managed infrastructure is ISO27001 accredited including secure media disposal** **Project reserves the right to witness the deletion of data first hand.** **Data destruction from Black Pear during the provision of services is possible (i.e 8 years after a patient in EPACCS has died).**

DPIA06 FORM: *TECHNICAL AND SECURITY MEASURES*

T1	What business continuity plans are in place in case of data loss or damage? (As a result of human error, virus, network failure, theft, fire, floods etc.)			**From Black Pear perspective – AWS SLAs are 99.95% availability supported by a robust BCDR plan.** **This does not take account of potential local network failures and local issues. Local reliance upon SIDeR will vary and need to be considered in organisational BCPs. SIDeR support will commit to informing partners of any identified failures and expected resolutions.** **SCW provided reverse proxy server is actually two servers to ensure capacity and a degree of resilience**
T2	What are the physical security measures have been undertaken to protect the data?			**The data is hosted in AWS Cloud services in secure data centres** http://www.redcentricplc.com/about-us/accreditations-frameworks/ https://aws.amazon.com/compliance/ **. Partner suppliers (AWS & Redcentric) are ISO27001 accredited (independent verification)** **Black Pear NHS Services are independently assessed via Cyber Essentials (IASME-A-05646) and subject to penetration testing and vulnerability assessment at least once a year.** **SCW Reverse proxy server is hosted in NHS infrastructure assessed to meet the requirements of hosting personal data (DSPT & Cyber Essentials Plus compliant). The server does not store personal data**
T3	Is there a usable audit trail in place for the use of the data? If yes, how often will the audit take place?	X	**Yes**	**Audit by Trust/SCC/ CCG/General Practice/Hospice IG lead(s) using reports to be built**
			No	
T4	Is the use of technology being considered? If yes, provide details of the internal IT Department stakeholder involved?	X	**Yes**	**Reverse Proxy Server to assist with request/response efficiency**
			No	
T5	Is the technology supported by the supplier or internal IT Department?	X	**Supplier**	
			IT Department	
			Neither	
T6	Could the technology change the way data is stored?			**Data in SIDeR is to be retrieved on demand for the main shared care record. For some use cases such as EPACCs data will be stored, but this is the approach from the start and not a change**
T7	What are the technical security measures have been undertaken to protect the data?			**Technical measures are in place within the Hosting services as set out in:** http://www.redcentricplc.com/about-us/accreditations-frameworks/ https://aws.amazon.com/compliance/ **Access to the system will be managed via a process to establish appropriate users and roles. User access**
	T4 – T7 not applicable (BUT IF T7 is general, then it will always be an applicable question?)			

				will be 'context launch' from their core system as SIDeR will then seek to retrieve data from the relevant source systems. Therefore user management of accounts will be dependent on their employing organisation's policy and processes as will items such as timeouts etc. Aventail and other software of choice, provided by Partner organisations will control device security and will wipe all data if compromised / deemed to be compromised by incorrect pin. Reverse proxy server is hosted on HSCN and all traffic is encrypted via HTTPS
T8	Is the use of cloud technology being considered? If yes, provide the data centre location:	X	**Yes**	**England (AWS England)**
			No	
T9	Is the cloud technology supported by the supplier?	X	**Yes**	
			No	
T10	Does the cloud hosting data centre(s) meet any standards such as tier-x standards to demonstrate cloud security? If so please provide details:			**AWS operates in alignment with Tier III+, but Black Pear have chosen not to have a certified Uptime Institute based tiering level – so they have flexibility to expand and improve performance. Black Pear do not claim Tier 4 alignment, but indicate this is where they would be if they did.**
T11	Could the cloud technology change the way data is stored?		**Yes**	
		X	**No**	
T12	How will the SIDeR data controllers be alerted to any possible cloud system breaches?			**Black Pear conduct their own monitoring of the infrastructure – actual or potential breaches are priority 1 escalation – conference call to the SIDeR CIO or nominated IG lead and repeat calls until incident closed.** **CCG to orchestrate following notification from Black Pear. If a local issue reported locally, all Partner organisations to ensure CCG are informed and involved in root cause and resolution call, so learning is cascaded to other Partner organisations.**
	T8 – T12 not applicable			
T13	Is the use of payment processing technology being used or considered? If yes, provide details of internal financial services stakeholder involved?		**Yes**	
		X	**No**	
T14	Is the use of payment processing technology supported by the supplier?		**Yes**	
		X	**No**	
T15	Is the use of mobile devices being considered?? If	X	**Yes**	

	yes, provide details of the internal IT Department stakeholder involved?		**No**
T16	Are the mobile devices supported by the supplier or internal IT Department?		**Supplier**
		X	**IT Department**
	T16 not applicable		**Neither**
T16	Could the project goals be achieved without processing personal data?		**Yes**
		X	**No**

T17	Could the project goals be achieved by using: (this assessment relates purely to Provision of Care use cases)				
	Pseudonymised data		**Yes**	**X**	**No**
	Anonymised data		**Yes**	**X**	**No**
	Aggregated data		**Yes**	**X**	**No**
	Statistical data		**Yes**	**X**	**No**

T18	If the use of personal data is necessary, compile the minimum array of personal data requited in order to achieve the project goals:	**This will be defined in a schedule for each use case.**
T19	How will users escalate cyber security, data security or data breaches in a timely manner?	Partner organisations' IT Helpdesks, escalated to IG teams

DPIA07 FORM: *SYSTEMATIC MONITORING, AUTOMATED DECISIONS AND PROFILING*

S1	Is the use of surveillance or CCTV being considered?	X	**Yes (if we consider use of audit trail)**
			No
S2	The aim of the surveillance or CCTV is:	X	**Protection of the human life and health**
			Protection of property
			Protection of employee life and health
			Control over the entry and exit from the official business premises
S3	Are there any other aims of the surveillance or CCTV?		**Control over employees**
		X	**Ascertaining diligence at work**
			Other

S4	Have you prepared the following:				
	Public notifications which are comprehensive, visible, positioned at the point the individual comes under surveillance		**Yes**	**X**	**No**
	Employee notifications which detail the surveillance in the official business premise.	**X**	**Yes** (Locally Trust / SCC policy)		**No**
	Adoption of a policy regulating the manner of performing surveillance	**X**	**Yes (above)**		**No**
	That no surveillance is used in dressing rooms, fitting rooms, toilets and bathrooms and other similar areas	**X**	**Yes**		**No**
S5	Does the employee notification's contain (all the below are related to informing that each partner already does for their staff – i.e. that access to systems will be monitored)				
	When surveillance is being performed	**X**	**Yes**		**No**
	Details of the controller performing the surveillance	**X**	**Yes**		**No**
	The purpose and period of preserving the images and recordings	**X**	**Yes**		**No**

S6	What is the retention period for the surveillance images and recordings?	**See NHS records management code of practice on Audit trail data.**
	S1 – S6 not applicable	

S7	Is the use of systematic monitoring of individuals being considered?		**Yes**
		X	**No**

S8	If systematic monitoring is being considered, please provide details of the monitoring that will take place including who, what, why and how often:		

S9	Is the use of systematic monitoring outcome involving decision-making?		**Yes**
		X	**No**

S10	If decision-making is envisaged, please provide details:		

S11	If decision-making is envisaged, will this interfere with the individual's freedoms and rights?		**Yes**
		X	**No**

S12	If systematic monitoring is being considered, have you prepared a document detailing the following:				
	Who will be monitored		**Yes**		**No**
	Why the monitoring will be conducted		**Yes**		**No**
	When the monitoring will be conducted		**Yes**		**No**
	Where monitoring will be conducted		**Yes**		**No**
	What will be looked for when conducting monitoring		**Yes**		**No**
	How to conduct monitoring		**Yes**		**No**
	Where the monitoring data will be stored		**Yes**		**No**
	Who will access the monitoring data		**Yes**		**No**
	Details of any decision-making from process		**Yes**		**No**

	S7 – S12 not applicable

S13	Is automated decision-making without human intervention being considered?		**Yes**
		X	**No (unlikely even with analytical developments)**

S14	If automated decision-making is envisaged, will it concern children or special categories of data?		**Yes**
		X	**No**

S15	If automated decision-making is being considered, is the individual able to:				
	Obtain human intervention		**Yes**		**No**
	Express their point of view		**Yes**		**No**
	Obtain an explanation of the decision and challenge it		**Yes**		**No**

S16	If automated decision-making is being considered, is this due to the any of the following conditions?				
	Necessary for entering into or performance of a contract between you and the individual		**Yes**		**No**
	Is authorised by law*		**Yes**		**No**
	*Law details:				
	Based on explicit consent		**Yes**		**No**

X ***S13 – S16 not applicable***

S17	will the evaluation “profiling” of certain personal aspects of an individual be carried out, such as:				
	Performance at work		**Yes**		**No**
	Economic situation		**Yes**		**No**
	health		**Yes**		**No**
	personal preferences		**Yes**		**No**
	reliability		**Yes**		**No**
	behaviour		**Yes**		**No**
	location		**Yes**		**No**
	movements		**Yes**		**No**
	Other:				

S18	If profiling is envisaged, please provide details of the mathematical or statistical procedures for the profiling:	

X ***S17 – S18 not applicable***

DPIA08 FORM: *DISCLOSURE AND SHARING*

D1	Will the project change the medium disclosure of publicity available information?		**Yes**
		X	**No**
D2	Will the project facilitate transferring or disclosing information to a country or territory outside of the European Economic Area?		**Yes**
		X	**No**
D3	Will the project by any means disseminate information to third parties?	X	**Yes**
			No
D4	If third party disclosure is envisaged has a non-disclosure agreement been executed?	X	**Yes (as information sharing agreements)**
			No
D5	If third party disclosure is envisaged, will services be provided in return for the disclosure and opportunity to release the information? If so please provide details:	No – this isn't the scope of info sharing that this project is focused on. The shared information will be utilised by partners, but it is not shared in exchange for service, but to facilitate better provision of existing service	
	D3 – D5 not applicable		
D6	Will the project by any means enable systematic sharing of information?	X	**Yes**
			No
D7	If systematic sharing is envisaged has an information sharing agreement been executed between the discloser and recipients?	X	**Yes**
			No
D8	If systematic sharing is envisaged, will services be provided in return for the sharing of information? If so please provide details:	Not in the way this is worded – see D5	
	D6 – D8 not applicable		
D9	Will any information or data be published on the internet or in other media types? If yes, please provide details:	X	**No**
D10	Will the project involve direct marketing?		**Yes**
		X	**No**

OUTCOME OF FULL DPIA

Following the evaluation of the DPIA01 form and declaration, a full data protection and privacy assessment was deemed to be necessary. The responsible project lead was notified that at this stage the Data Protection Officer (DPO) will now be involved and the DPO recommendation(s) and conclusions(s) must be integrated into the project plan before the project is developed and implemented.

Responsible project lead	[redacted]
Project name	**SIDeR (Somerset Integrated Digital electronic Records)**
Project or scheme reference number	
Estimated project completion date	**March 2021**

IDENTIFIED RISK(S)

1. **Risk of data being held in unsecure environment:** Data and apps are hosted in cloud environment via Amazon Web Services (AWS) & Azure and not in the local control of the data processors. Reverse proxy server managed on HSCN network, all traffic encrypted and does not store data.

2. **Data processed on individuals who are unaware of the processing:** This relates to activities to inform individuals of the use of their data across the SIDeR programme

3. **Unauthorised use of data by end users:** Where a user accesses information on individuals that they have no business related reason to access. This includes the risk of data on patients on the boundaries of Somerset being included as some organisations involved in sharing provide services over 'Somerset' boundaries

4. **Sharing & recording of inaccurate data:** A number of the SIDeR initiatives feature the creation of data collection forms as well as extracts of data from other sources.

5. **Data retained for longer than is necessary:** Unless properly managed data may be retained on systems and potentially accessible for longer than is necessary in breach of Data Protection Principles. This is both in terms of data held for the duration of the contract and for the general retention of data for health & social care records.

6. **Unavailability of data due to:**

    a. **System failure:** resulting in poor service delivery due to lack of information
    b. **Poor system design:** Where data required is either not included in exchanges or not available to end users due to poor role based access or screen design

7. **Failure to report data breaches to regulator/data subjects:** Most data breaches are now required to be reported to the Information Commissioner's office, and those presenting a high risk should be reported to the affected data subjects. Failure to comply may result in significant time loss dealing with action or aggravation for any potential regulator action.

8. **Unlawful sharing of personal data:** The programme is fundamentally about sharing data for effective provision of care across the health & social care community and this has to be done by appropriate legal gateways and lawful basis for processing data. There is a risk that uses of data

are not properly assessed and that data will be shared unlawfully, which risks regulatory action, data subject complaint and potential financial and reputational impacts on the programme.

RECOMMENDATION(S)

1. **Hosting environment –** AWS & Azure are accredited providers of cloud services to the public sector and have achieved ISO27001(certificate provided). There is significant technical detail in the response to the tender that has been reviewed by the Technical Workstream and assessed as a reasonable level of security and no more detailed analysis is required. Reverse proxy server (which doesn't store data) established on HSCN network with all traffic handled encrypted.

2. **Informing individuals** – the programme has a communications workstream including the articles in Your Somerset (i.e. https://somersetnewsroom.files.wordpress.com/2019/12/taunton-deane-winter-2019.pdf). Each 'use case' will in the appendices for the DPIA and Information Sharing Agreement identify any specific informing of individuals that is required and how it will take place. A core website containing public facing details about SIDeR activities is set up in the CCG website: https://www.somersetccg.nhs.uk/about-us/digital-projects/sider/ to support informing requirements in a consistent manner. The IGWG discussed and agreed in June 2019, that the use of Amazon Web Services and Azure does not meet the definition of an 'international organisation' in GDPR article 4, so there is not a specific need to inform data subjects of the information being processed by these organisations, particularly as much of the data does not persist in this architecture. All partners are required to include reference to SIDeR in their organisational 'fair processing/privacy notice'. In addition staff will be guided to inform users about accessing their SIDeR SCR when they are face to face with a patient/client.

3. **Unauthorised access –** The system will operate a number of access controls (i.e. username/password, password refresh/complexity, timeouts – via organisational systems and 'context launch' into SIDeR) and also have controls based around the roles of staff and care relationships with data subjects as well as education and training of end users being a key element of the 'qualifying standard' (DS&PT compliance) for an organisation to join the partnership. These will be managed by robust user request/approval/management and revocation procedures as currently operated by each partner to their operational systems consistently. It is also recommended that regular audit reports are run and checked with all partners agreeing what auditing is effective to undertake.

   Should any audit report identify potential inappropriate access that will be managed via the existing policy of the staff members employing organisation.

   Should any partner identify or have reported to them potentially inappropriate access by staff who are not their employees, they will raise this with the employing organisation to lead an investigation at the earliest convenience, following their organisation policy on such matters. This will be considered as a breach as set out in section 12 of the ISA.

   Some partners provide services beyond the boundaries of Somerset (i.e. YDH activity is 85% Somerset) . Any such patient will not be excluded on the basis that:
   - Other agencies participating may also see such individuals and have justifiable reason to access
   - If there is no need for any patient's data to be accessed (both within Somerset and cross border) then it should not be. Any inappropriate access is reduced by controls such as training, context launch (i.e. if the patient isn't in the source system, they won't be accessed), employment contracts
   - The model for SIDeR means the data on 'out of area' patients is not sitting in a repository waiting to be accessed

4. **Data Accuracy –** Data validation processes need to be built into each development, whether the data is extracted from other systems or captured at source. Each data capture system will be

carefully set up to capture coded data where possible and apply data field controls to ensure appropriate entries are made. Each development must be subject to a testing phase before going live.

5. **Data Retention –** Assurances are in place from Black Pear that on termination of service a copy of all data will be transferred to the data controllers (securely) and deleted from the service infrastructure within 30 days. The infrastructure is cloud based, provided by AWS and Azure and is likely to have appropriate deletion processes, but the nature of the service is the storage area will be reused by the provider rather than the hardware decommissioned and destroyed. If any data controller requires further assurance on deletion of data from AWS, then this can be researched, but if all D/Cs are happy then the resource to do this need not be spent. It is also noted that large amounts of data to be used via SIDeR will not persist to be stored in the system as it is retrieved on request, displayed and then not kept in the system. In addition the programme will establish retention periods for any data captured and shared, such as EPaCCS, in line with the records management for health and social care records.

6. **Unavailability of data**

    a. **System failure –** Black Pear have provided detail on SLAs for up time of the systems (99.95% availability). However there are other points of failure, such as local networking that can cause unavailability. Initially reliance on SIDeR applications will not necessarily be critical to service delivery, so the risk and impact is relatively low. Previous methods of finding and sharing data (phone calls/emails) can be used. Options for fallback in the absence of the system (for any reason and any scale) are limited. As use becomes more critical this will have to be addressed in each use case DPIA appendix. Reverse proxy server is actually two instances to handle capacity and provide resilience.

    b. Poor system design – Data requirements for each use case will identify the data that is necessary for the use case and which roles need access to it. These requirements will be defined and agreed with representatives from the relevant professional groups involved. Screen designs to ensure that pertinent data is clearly visible will also be tested.

7. **Failure to report data breach –** Black Pear have provided assurance about monitoring the infrastructure for actual or potential breaches and how they will escalate these. The programme need to determine shared procedures for identifying, reporting and managing data breaches related to the SIDeR applications.

8. **Unlawful sharing of data –** This is addressed by the assessment of the data sharing proposals and establishing the appropriate legal gateway and lawful basis for processing. This is being managed by the establishment of a SIDeR Information Sharing Framework. This consists of a core ISA linked to the Somerset Overarching Information Sharing Protocol (SOISP) that details the legal gateways, lawful basis, the responsibilities of partners as data controllers and data processors (e.g SoftCat, Black Pear). The ISA also sets out key principles around informing, data quality, access controls, qualifying standards (for participation). The core ISA will be supplemented with appendices on use cases/work programmes where there is a difference for any particular use case from the core document. Any areas where there is lack of clarity or agreement, expert advice will be utilised as well as engagement with the Information Commissioner's Office.

FINAL CONCLUSION(S)

1. **Hosting environment – likelihood of incident is low. Impact of an incident will grow as usage of the applications in SIDeR grow. Conclusion is to consider periodic review based on programme development.**

2. **Informing individuals – As long as the focus on this angle is not lost during the design and implementation phases of each use case, then the risk of individuals being poorly informed is low. This will need monitoring by the IG Working Group and potentially testing with patient/service user representatives.**

3. **Unauthorised access – proper specification and implementation of the access controls and processes will ensure that inappropriate access is a low likelihood of occurrence. Impact would vary on the level of unauthorised access and the intent of the staff member.**

4. **Data Accuracy – careful and considered development of forms, validation of extracts and testing are reasonable controls to reduce the risks from inaccurate data. However it will not eliminate it and staff must be encouraged to highlight and seek to correct inaccuracies.**

5. **Data Retention – Assurances from the supplier of provision of a copy of data on termination to the data controllers and secure removal from the infrastructure look reasonably credible to identify the risk of data being retained longer than necessary (and in particular beyond contract length) on the infrastructure is low. The risk of the programme storing data for longer than necessary can also be noted as low if the programme identifies the relevant retention periods for data in each use case.**

6. **Unavailability of data:**

    a. **System Failure – risk currently identified as low probability and low impact, although as usage grows the impact of failure will become a higher impact issue**
    b. **System design – provided the data needs are clearly defined and agreed with the relevant staff and the developments appropriately tested this will be low probability and low impact**

7. **Failure to report data breach – Black Pear response is reassuring. Provided the programme develop and agree (and audit) incident identification and response process, then the risk of failing to report appropriately is low.**

8. **Unlawful sharing of personal data – Finalisation, sign up and monitoring of the requirements of the ISA & appendices will reduce the risk of unlawful processing of data to being classed as 'rare'.**

NB – Organisational risks for connecting to SIDeR will be managed and mitigated by the technical group, overseen by the IG working group.

Specific risks – added after initial DPIA work concluded:
Use of deceased records for testing – this is where a small number of records of individuals who have had care in multiple organisations are to be used for system testing. The real identity of these patients is removed and replaced with a false identity, so that the data does not, and never has related to a specific living individual. This process has been discussed in the IG working group, the technical workstream and the Digital Delivery Board and accepted as an appropriate way to create test data

By signing this DPIA outcome form, the responsible project lead confirms that they have read and understand the identified risk(s), sources of risk(s), recommendation(s) and conclusion(s) provided by the DPO. The responsible project lead is under no statutory obligation to accept such recommendation(s) and conclusion(s) however under these circumstances, unaccepted arrangements must have a rationale and be escalated to the ICO and SIRO.

ACCEPTED The recommendations and conclusions will be integrated into the main project plan and actioned appropriately.

NOT ACCEPTED The recommendations and conclusions will be integrated into the main project plan. However, they will not be accepted or actioned due to the following rationale:

Risks are accepted on recommendation of the IG Working group and the DPIA documentation being available to all data controllers.

Signed and dated:	**(not applicable – see above re IGWG)**