St Helens & Knowsley NHS
Health Informatics

Data Protection Impact Assessment

(DPIA)

General Data
Protection Regulation

Data Protection Act
2018

Instructions for Completing this DPIA

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project or change in the way personal data is processed. This is a mandatory requirement under the General Data Protection Regulation (GDPR).

As a pre-cursor to completing a DPIA, it is the responsibility of the Project Manager to ensure that the Due Diligence Questionnaire Due Diligence Questionnaire 20-21. is completed by any 3rd party who are providing the product/service/solution and is approved and signed by a Deputy Director of Informatics in advance of completing a DPIA. Furthermore all new projects or changes must be discussed and approved at the Change Advisory Board (CAB) that meets weekly.

Sections 1 to 9 - to be completed by the Project Manager, Information Asset Owner (IAO), Information Asset Administrator (IAA)

Sections 10 and 11 - to be completed by a member of staff from the IG Lead or Senior IG Lead in conjunction with the IAO or IAA

Section 12 - requires review of all items entered of the Data Protection Officer and Information Security Officer before being sent to the Senior Information Risks Owner (SIRO) for final sign-off.

1: Basic Information

Reference (IG to complete):

DPIA Title (PM to provide): St Helens Shared Cares Record

DPIA Completer Name:*(please note this should be the Project Manager with the IAO / IAA*	Kirsty Brown
Department:	Mid Mersey Digital Alliance
Email:	
Telephone No.:	
New System / Process Name:	St Helens Shared Cares Record
New System Supplier Name: (if applicable):	Graphnet Health Ltd and System C Healthcare Limited
Date System due to go live (if applicable):	The system went live November 2018. This DPIA is a review of the existing DPIA for St Helens Cares.
Project Proposal / Purpose for completing DPIA:	St Helens Cares seeks to further develop person centered services and support, delivered to patients in St Helens Borough. The proposed solution will enable the integration of information from a number of sources, relating to the care of patient and enable this information to be viewed by authorised health and social care professionals involved in the care of that individual. Access to a St Helens Cares Record will enable improved seamless care to patients registered with any GP Practice in St Helens Borough. It is anticipated that this will reduce needless admission to hospital and bring care closer to home. There is the potential to reduce untoward incidents as history of certain interventions will be available to all professionals who are involved in the individual's care.

Embed the approval minutes from the CAB:	St Helens Cares have been discussed with key stakeholders prior to the roll out date of the project. This initiative has been approved by all parties involved and progress of this initiative is closely monitored by St Helens Cares Information Governance Steering Group.
Embed the approved security Questionnaire:	

2: Screening Questions

Documenting here which of the screening questions are applicable to your initiative will help to draw out the particular privacy considerations that will help formulate your risk register later in the template

	Yes	No	Unsure	**Comments -** *Document initial comments on the issue and the privacy impacts or clarification why it is not an issue*
Is the information about individuals likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?		x		Information will be shared with organisations involved with the St Helens Cares project on a need to know basis. Patients are aware that their information can be shared with other professionals as part of their direct care. Only authorised staff can access the shared care record and activity on the system is time and date stamped. Professionals accessing the shared care record are bound by duty of confidentiality
Will the initiative involve the collection of new information about individuals?	x			The initiative involves the collection of new information about patients for certain members involved with St Helens Shared Care Record initiative.
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	x			Currently, some parties to this agreement might not have access to certain information of patients registered with GP Practices in St Helens. The shared care record will enable organisations to share, process and collect data of patients registered with St Helens GP Practice in order to provide professional support. Information will also be processed to enable effective management of the health conditions of patients registered with St Helens GPs.
Will the initiative require you to contact individuals in ways which they may find intrusive[1]?		x		Patients will be contacted from time to time by professionals as part of their direct care. However, this is not perceived as being intrusive as professional will have to initiate contact with the patients in order to effectively manage them.

Will the information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	**x**			Currently, some parties to this agreement might not have access to certain information of patients registered with St Helens GPs. This initiative will enable organisations to share process and collect data of patients in order to provide professional support. Information will also be processed to enable effective management of the health conditions of patients in St Helens.
Does the initiative involve you using new technology which might be perceived as being intrusive? e.g. biometrics or facial recognition	**x**			The technology used for hosting St Helens Shared Cares is new to this initiative. Information will have been recorded on the systems by individual organisations. Certain parties to this initiative do not access to the system or certain information hosted on the system. The technology is needed to host clinical data and is not perceived as being intrusive.
Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	**x**			Authorised professionals with access to St Helens Shared Care Record will be able to access and review clinical information as part of the direct care of patients registered with St Helens GPs in order to make informed decisions.
Will the initiative compel individuals to provide information about themselves?	**x**			Patients will be required to provide certain information about themselves and their health in order to receive treatment and professional support. Information will only be obtained from patients when they come in contact with the Trust or other partner organisation.

If you answered **YES or UNSURE** to any of the above you need to continue with the Data Protection Impact Assessment.

***Sign off if no requirement to continue with Data Protection Impact Assessment*:**

Confirmation that the responses to a – h above is NO and therefore there is no requirement to continue with the Data Protection Impact Assessment

Agreed by: ___________________________________name of group or individual(s).

3: Contact Information

Project Management Details	
Project Manager:	Kirsty Brown
Project Manager Email:	
Project Manager Telephone No.:	
Information Asset Owner (IAO) Details	
Information Asset Owners are directly accountable to the SIRO and must provide assurances that information risk is being managed effectively in the respect to the information assets that they 'own'.	
IAO Name:	Christine Walters
IAO Title:	Director of Informatics
IAO Department:	Mid Mersey Digital Alliance
IAO Email:	
IAO Telephone Number:	
Information Asset Administrator (IAA) Details	
Information Asset Administrators are usually members of staff who are familiar with and have knowledge of the information held, information risks and information systems within their department. They know how their systems work and who should have access to the data held within them.	
IAA Name:	Kirsty Brown
IAA Title:	Shared Care Record Manager
IAA Department:	Mid Mersey Digital Alliance
IAA Email:	
IAA Telephone Number:	

Link to wider initiative *(if applicable)***:**	In November 2014, the National Information Board (NIB) published a framework for action ‘Personalised Health and Care 2020’, outlining their vision for joined up, digital real-time records, data standards, intelligence and patient access to records across care settings.		
Information Technology Involvement	List any applicable electronic systems/software to this initiative (current and/or new):		
	System name	**Used by e.g. organisation and dept.**	**Parties/system supplier**
	CareCentric	StHK and other organisation involved with the St Helens Shared Cares Record project	System C Healthcare Limited and Graphnet Health Ltd
	Medway Live	StHK	System C
	Liquid Logic	St Helens MBC	System C
	RIO	Northwest Borough NHS Trust	Servelec Ltd
	EMIS	GPs	EMIS
	Vision Health	GPs	Cegedim healthcare solutions
	SystemOne	St helens Urgent Treatment Centre	The Phoenix Partnership
Are any other organisations are involved in this initiative?	Yes – List of organisations can be found on the data sharing agreement		
Confirm all relevant organisations have or are working towards Cyber Essentials. ***Cyber Essentials is a Government-backed, industry-supported scheme to help organisations protect themselves against common online threats.***	**Organisation/Parties/ system supplier**	**Cyber essentials Y/N Working towards/cyber compliance defined under terms of contract**	
	Graphnet Health Ltd	Y – See due diligence	
	System C Healthcare Limited	Y – See due diligence	

Is this initiative in line with or achieving national or local guidance/ strategy or mandate?	St Helen Shared Cares Record is a local strategy aimed at providing 5 star patient experience to Patients registered with St Helens GP Practice by creating a platform where organisations can access personal and clinical information in order to effectively manage St Helens patients.

4: Personal Identifiable Data Items

Data Item	Description	Specific Data Item(s)	Justification Reason that the data item(s) are needed - Caldicott justification
Personal Details	Information that identifies the individual and their personal characteristics	Check all that apply: ☒ Forenames(s) ☒ Surname ☒ Address ☒ Postcode ☒ Date of Birth ☒ Age ☒ Gender ☐ Physical Description ☒ Home Telephone Number ☒ Mobile Telephone Number ☒ Other Contact Number ☒ Email Address ☒ GP Name and Address ☒ Legal Representative Name (Next of Kin) ☒ NHS Number ☐ National Insurance Number ☐ Photographs / Pictures of persons ☐ Other – if this is ticked please list other personal data items to be processed below ☐ See Attached	**To allow for effective management of patients registered with St Helens GPs** **Principle 4: Access to personal confidential data should be on a strict need-to-know basis** Only those who need access to personal confidential data should have access to it. They should also only have access to the data items that they need. **Principle 5: Everyone with access to personal confidential data should be aware of their responsibilities** Action should be taken to ensure that those handling personally identifiable information are aware of their responsibilities and their obligation to respect patient and client confidentiality. **Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality** Health and social care professionals should have the confidence to share information in the best interests of their patients and within the framework set out

			by these principles. They should also be supported by the policies of their employers, regulators, and professional bodies.

What data items are being processed e.g. for collection, storage, use and deletion: if there is a chart of diagram to explain please attach as an appendix

Data Item	Description	Specific Data Item(s)	Justification Reason that the data item(s) are needed – this must stand up to scrutiny for Caldicott justification
Physical or Mental Health or Condition	Information Relating to the individuals physical or mental health or condition NB. For mental health this would include the mental health status i.e. whether detained or voluntary under the Mental Health Act	☒ Yes ☐ No ☐ Not Applicable List any data items below or attach as an appendix	Principles 4,5 and 7 as stated above
Sexual Identity and Life	Information relating to the individuals sexual life	☒ Yes ☐ No ☐ Not Applicable ☐ List any data items below or attach as an appendix	Where applicable this information may be present on the Care Record (GP demographics).
Family Lifestyle and Social Circumstances	Information relating to the family of the individual and the individuals lifestyle and social circumstances	☒ Martial / Partnership status ☒ Carers / Relatives ☒ Children Dependents ☒ Social Status – e.g. Housing	Principles 4,5 and 7 as stated above

		☐ Not applicable ☐ Other – please specify below:	

What items are being processed e.g. for collection, storage use and deletion: if there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific Data Item(s)**	**Justification Reason that the data item(s) are needed – this must stand up to scrutiny for Caldicott justification**
Offences including Alleged Offences	Information relating to any offences committed or alleged to have been committed by the individual	☐ Yes ☒ No ☐ Not Applicable List any data items below or attach as an appendix	
Criminal Proceedings, Outcomes and sentences	Information Relating to criminal proceedings outcomes and sentences regarding the individual	☐ Yes ☒ No ☐ Not Applicable List any data items below or attach as an appendix	
Education and training details	Information which relates to the education and any professional training of the individual	☐ Education / training ☐ Qualifications ☐ Professional Training ☒ Not applicable ☐ Other – please specify below: Click here to enter text	Click here to enter text

What data items are being processed e.g. for collection, storage, use and deletion: if there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification Reason that the data item(s) are needed – this must stand up to scrutiny for Caldicott Justification**
Employment Details	Employment and career history	☐ Employment status ☐ Career details ☒ Not applicable ☐ Other – Please specify below Click here to enter text	Click here to enter text
Financial Details	Information relating to the financial affairs of the individual	☐ Income ☐ Salary ☐ Benefits ☒ Not applicable ☐ Other – Please specify below Click here to enter text	
Religious or other beliefs of a similar nature	Information relating to the individuals religion or other beliefs	☒ Yes ☐ No ☐ Not applicable List any data items below or attach as an appendix	

<table>
<tr><td colspan="4"><b>What data items are being processed e.g. for collection, storage, use andf deletion</b>: if there is a chart or diagram to explain please attach as an appendix</td></tr>
<tr><th>Data Item</th><th>Description</th><th>Specific data item(s)</th><th>Justification reason that the data items are needed – this must stand up to scrutiny for Caldicott Justification</th></tr>
<tr><td>Trade Union Membership</td><td>Information relating to the individuals membership of a trade union</td><td>☐ Yes
☒ No
☐ Not applicable
☐ List any data items below or attach as an appendix</td><td></td></tr>
<tr><td colspan="4"><b>You must confirm that the data items you have ticked above are relevant and necessary to your project and there is a justified reason for it – if they are not you must amend the above selection to remove those items not relevant / necessary</b></td></tr>
<tr><td colspan="4">✓ Confirm</td></tr>
</table>

5: Legal Basis for Processing the Data

Is the initiative for delivering Direct Care?

The definition of direct care is: A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes:-

- *supporting individuals' ability to function and improve their participation in life and society*
- *the assurance of safe and high quality care and treatment through local audit,*
- *the management of untoward or adverse incidents*
- *person satisfaction including measurement of outcomes*

undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care

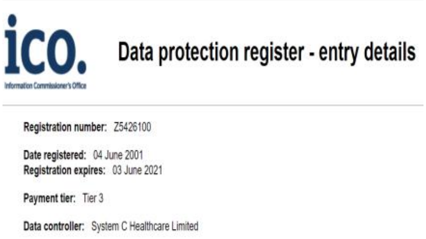
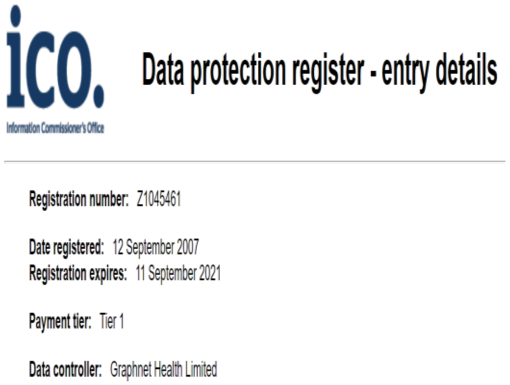
1a If not Direct Care, what is it delivering and how is the consent being obtained	Indirect Care ☐ Commissioning ☐ Monitoring Health and social care - Information will also be processed to enable effective management of the health conditions of patients in St Helens. ☐ Public health ☐ Research ☐ Other – specify ……
1b What is the legal basis that permits you to carry this out for indirect care	Legal basis ☐ Explicit consent ☐ Section 251 ☐ Other legal gateway – specify - Article 6(1)(d) & (e) Article 9(2)(c), (h) & (i)
1c Is there a facility for the patient to opt out of their data being processed?	☐ No ☒ Yes If yes, please describe how this process will be managed? Data subject to contact practice for further discussion with GP before opt out will be considered.

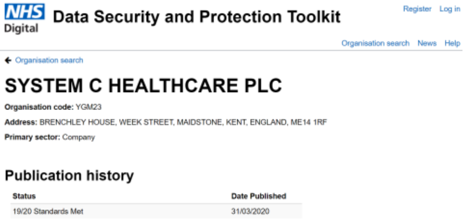
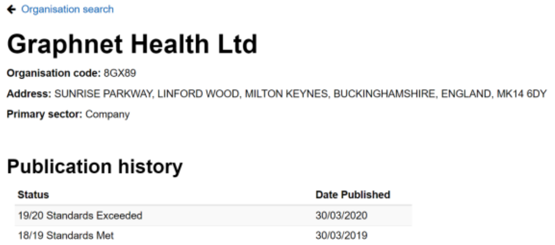
✓ ☐ **Yes (go to Q2)** ☐ **No (go to Q1)**

2 Informing Individuals: Please state how patients and / or staff will be informed / have been informed of the data collection and processing?	Patients are informed via the Trust patient privacy notice http://www.sthk.nhs.uk/about/how-we-use-your-information/privacy-notices Parties to this agreement also notify patients through their patients privacy notice on their website and noticeboards Graphnet Privacy Notice - https://www.graphnethealth.com/privacy/privacy-policy-for-end-users/ System C Privacy Notice - https://www.systemc.com/legal-information/privacy-policy/		
Information Sharing within UK: Will personal confidential data be shared with any other organisation?	☒ Yes – There is a data sharing agreement for this initiative which outline the responsibilities of each organisations. The data sharing agreement contains standard data protection clauses. ☐ No		
If yes, please state who the information will be shared with and how and enter in the table	From originator Organisation	Data sent to via:	To Receiving Organisation:
If yes, please state who the information will be shared with and how and enter in the table Is the information from receiving organisation sent back to originating organisation? If yes, please state how the information is transferred back and enter in the table:	St Helens Shared Cares Record - Flow (	CareCentric	All partner organisation that are parties to this agreement.
Is the information from receiving organisation sent back to originating organisation? If yes, please state how the information is transferred back and enter in the table:	From Receiving Organisation:	Data sent back via:	To Originating Organisation
	As per above		

Will Personal Identifiable Data be sent outside the European Economic Area (EEA)? If yes, please state who the data will be sent to and how?	☐ Yes ☒ No, data will be processed in the UK. ☐ Not Applicable Please enter text here
Have data protection checks been undertaken to ensure that the non EEA country has adequate data protection / information security standards in place? If yes, please state what checks have been made:	☐ Yes ☐ No ☒ Not Applicable – Data will be processed in the UK and appropriate due diligence checks have been carried out on the suppliers. Please enter text here
Sending data to the USA?	☐ Yes ☐ No ☒ Not Applicable ☐ Yes ☐ No

6: Information Asset / System Information

Please enter the Security Questionnaire by embedding the completed documents in this section. This must be signed off by the Information Security Officer.		Appropriate due diligence have been carried out on Microsoft who are the cloud provider by NHS Digital prior to the roll out of a different project (NHSmail) Https://digital.nhs.uk/services/nhsmail/nhsmail-to-launch-hybrid-service-with-office-3 Microsoft have published blue prints specifically for different industries, health being one. We have used these blueprints as a basis of our cloud deployments.	
ICO Notification: If a system is being used, is the Supplier (of this system) registered with the Information Commissioners Officer (ICO) https://ico.org.uk/ESDWebPages/Search If yes, please state their registration number:	☐ Yes ☒ No ☐ Not Applicable  Data protection register - entry details Registration number: Z5426100 Date registered: 04 June 2001 Registration expires: 03 June 2021 Payment tier: Tier 3 Data controller: System C Healthcare Limited Please enter text		 Data protection register - entry details Registration number: Z1045461 Date registered: 12 September 2007 Registration expires: 11 September 2021 Payment tier: Tier 1 Data controller: Graphnet Health Limited
DSP Toolkit: Has the Supplier / Third Party completed a Data Security and Protection Toolkit Assessment (formally IG toolkit check here: https://www.dsptoolkit.nhs.uk/OrganisationSearch and / or had a ISO27001 accreditation Please describe the scope for ISO 27001	DSP Toolkit completed: ☒ Yes ☐ No Graphnet uses Microsoft Azure Data Centres to store and process data, with both (UK South and UK West) being sited	DSP Toolkit audited: ☐ Yes ☒ No	ISO 27001 Accreditation: ☒ Yes ☐ No

	in the UK. This platform meets ISO/IEC 27001/27002:2013, HIPAA and FedRAMP. Microsoft is certificated to the ISO/IEC 27017 - 27018 security control standards
	Please enter text here  NHS Digital Data Security and Protection Toolkit Register Log in Organisation search News Help ← Organisation search SYSTEM C HEALTHCARE PLC **Organisation code:** YGM23 **Address:** BRENCHLEY HOUSE, WEEK STREET, MAIDSTONE, KENT, ENGLAND, ME14 1RF **Primary sector:** Company Publication history **Status** – **Date Published** 19/20 Standards Met – 31/03/2020  ← Organisation search Graphnet Health Ltd **Organisation code:** 8GX89 **Address:** SUNRISE PARKWAY, LINFORD WOOD, MILTON KEYNES, BUCKINGHAMSHIRE, ENGLAND, MK14 6DY **Primary sector:** Company Publication history **Status** – **Date Published** 19/20 Standards Exceeded – 30/03/2020 18/19 Standards Met – 30/03/2019
Contract: Has the third party signed the relevant contract (containing the Information Governance clauses) e.g. NHS E contract / SLA with IG Clause	☒ Yes – Contract contains standard data protection and security clauses ☐ No
If yes, please state which contract type they have signed up to:	Service Level Agreement with Data Protection Clauses.

Asset / System Operation: Does this asset use privacy invasive technologies for staff and / or patients, e.g. Smartcards? If yes, please state the technology being used:	☐ Yes ☒ No – Authorised professionals from partner organisations can access the system with their AD Login, SmartCard or user name and password created by the Shared Care Record Team. Access to the system by these means is not perceived to be invasive. Please enter text here:
Will the asset / system process different personal confidential data items which have not been processed previously? If yes, please state the new personal confidential data items to be processed:	☐ Yes – ☒ No – The system will process personal data already processed by partner organisations. Please enter text here:
Will the asset / system involve new or changed identity authentication requirements that may be intrusive for staff and / or patients? If Yes Please state the new identity authentication requirements:	☐ Yes ☒ No – Authorised professionals will be authenticated via their login details or SmartCards through their source systems in most cases. However certain users will be log in using user name and password created by the Shared Care Record Team. Please enter text here:
Marketing: Will the asset / system send marketing messages by electronic means?	☐ Yes ☒ No

If yes, please state what you are intending to send for marketing purposes:	N/A
Have individuals been informed of the marketing and the option to opt in to this?	☐ Yes ☐ No ☒ N/A
Automated Decision Making: Is automated decision making to be used within the asset / system? If yes, please briefly describe the process and the reason for it?	The system does not have the capacity to make automated decisions. Decisions regarding patients care and welfare will be made by appropriate health professionals involved in the direct care of their patients.

7: System Security, Functions & CLOUD – only to be completed for systems / software

Pseudonymisation / Anonymisation: Can personal confidential data be anonymised or pseudonymised using the system / asset?	☐ Yes ☒ No – Authorised professionals from partner organisations will require access to personal and special categories data to be able to manage patients across St Helens Borough.
Data Quality: How will the personal confidential data be kept up to date and checked for accuracy?	All partner organisations have in place their own Data Quality Policy. Quality checks are carried out to ensure data held on the system are accurate and up-to-date. Data quality issues are escalated to the IG at that organisation. Data quality incidents are also reviewed and discussed at St Helens Shared Cares Information Governance Steering Group.
Access: Who will have access to the system and the personal confidential data? How will access be controlled?	Authorised professionals from partner organisations will be granted specific access rights according to their role and organisation. End user passwords are required to be complex and a minimum of 8 characters, and subject to the Trust and Partner's Password Management Policy. This is enforced through Active Directory Policy. The suppliers can also access the system to help investigate and solve issues as stipulated in the contract in place for managing the system. In some instances health professionals or partners will access patient information on the request of other professionals e.g. a GP may contact a social worker regarding a patient and the social worker will access the record. Passwords of technical support staff employed by the suppliers typically have 16 characters in length and include a minimum requirement for numeric and non-alphabetic characters and are typically changed every 3 or 6 months • Access control is at the core of the Information Sharing Agreement and this uses role and service based profiles and legitimate relationships. This means that care professionals will only gain access to information deemed necessary, proportionate and relevant to their role, setting of care and to the care of the individual. • The below table shows a high level summary of each of the role / service profiles that have been identified as part of the Information Sharing Agreement. It also shows the associated levels of access each profile

will have across to each segment and tier of the Information Sharing Model.

Professional Group	Sub-Category	Levels of access
1. Medical	1a. Hospital Specialist	S3, C2, D3, H3
	1b. GP	S3, C3, D3, H2
	1c. Community Medical	S3, C2, D3, H2
2. Registered Health Care Professional	2a. Specialist (e.g. Matron)	S3, C2, D2, H2
	2b. Generalist (e.g. Allied Health Professional)	S3, C1, D1, H1
3. Social Care Professional	3a. Hospital	S3, C1, DX, H2
	3b. Community	S3, C2, DX, H1
4. Unregistered Professional	Nil (e.g. Support Worker, Health Trainer, Auxiliary Nurse)	S3, CX, DX, HX
5. Admin / Clerical	Nil	S1, CX, DX, HX
Service Area		
6. Urgent Care	E.g. AED, WIC, AMU etc	S3, C1, D3, H3
7. Extended Primary Care Team	E.g. GP, Community Matron, District Nurse, Practice Nurse	S3, C3, D2, H2

- The St Helens Cares Record takes data as described above from source systems and re-presents it to care professionals in context within their organisations.

- If a non-standard role is required this would be discussed at the information Governance group and authorised by the Shared Care Record Steering board

Auditing:

Is there an audit trail for the system?

Please can you describe briefly how the audit trail works?

☒ Yes – Users activities can be audited when required. The system is time and date stamped.
☐ No

Audits can be carried out for those organisations that have viewed data are three audit properties which are accessible based on an individual’s role (RBAC process):

- **AuditActionUsage**
- **AuditEntity**
- **AuditEntityProperty**

AuditActionUsage table stores all the information about every action which were accessed by the user. It includes,
Audit ID
Action Name,
Controller Name,
Action Type (GET, PUT, POST, DELETE),
User who accessed
Time Stamp and Status columns.

AuditEntity
This table stores information about Entity Added/Modified/Deleted. Here **AuditID** is Foreign Key from **AuditActionUsage** table. For every row in this table there will be a reference in **AuditActionUsage** table. Since this table stores information about Entity Added/Modified/Deleted so if there is a GET call where no entity was Added/Modified/Deleted then we will not get any entry in **AuditEntity** table. Here **AuditEntityID** is primary key and for every **AuditID** from **AuditActionUsage** table that has ActyionType other than ‘GET’, it will have as many rows as number of entities Added/Modified/Deleted during that controller action execution. This tell gives information about which Entity from which Database was involved and what was action taken on the entity.

AuditEntityProperty
This table stores information about all properties for an entity whose values were Added/Modified/Deleted. It has **AuditEntityID** as Foreign Key from **AuditEntity** table. For every **AuditEntityID** in **AuditEntity** table, it will have as many rows as number of properties values Added/Modified/Deleted during that controller action execution. This table will show which properties were modified and what was old and new value.

Organisations are able to raise a request with the Graphnet Service desk should they require any specific audit requirements.

Storage of data: Where will the system information be stored securely?	☐ Within a paper based system stored securely ☒ Within a system / application stored on secure network ☒ Within a database / spreadsheet stored securely on network ☐ Other If Other, please state:
Back Up: Are there secure and reliable back up processes in place for the data stored on the system? If yes, please briefly describe what these are and that they will be fit for business continuity following a system failure *Please note you may need to contact IT Services for guidance regarding this question*	☒ Yes Graphnet - Data is backed up using the Azure Point in Time service. System C - Data are backed up as part of the contracted managed service or using the Azure Point in Time service for our cloud based services. ☐ No

Retention: Please state the retention periods for the information processed in the system? Please refer to the Records Management: NHS Code of Practice for Health & Social Care 2016 for assistance with this.	Records are retained in line with the NHS Code of Practice for Health & Social Care 2016. The 'data' feed will be reviewed annually by the Clinical Design Authority to ensure that the content of the STHCR is appropriate for its intended use. Data that is no longer deemed to be relevant will be cleansed from the STHCR. The audit log will be retained for ten years. See clause 10 on the data sharing agreement.
Disposal: How will the personal identifiable data be disposed of when this is no longer required.	Records are securely disposed of in line with the contract, NHS Standards and data protection legislation
Training: Each party to confirm that information governance training is in place and all staff with access to personal data have had up to date training	☒ Yes – All staff will be expected to undertake annual mandatory training in Information Governance and working within a shared record environment. (This is included as part of the annual Data Security Protection Toolkit submission). • There is a full-time trainer/tester working within the St Helens shared care record team, all new users are provided with training and training materials. • Regular engagement and training is also embedded into local induction programmes along with regular on-going support. • System support is accessible via IT Service desk telephone number or email. • Training Materials and guides can be found on the Intranet. Assurances from both suppliers - Staff receive Information Governance (IG) and Information Security (IS) inductions as well as receiving annual IG and IS training. ☐ No
Will clinical data be hosted within the Cloud application?	☒ Yes ☐ No ☐ N/A – Go to Q8

Is the Cloud data hosting service within the European Economic Area (i.e. the European Union or Norway, Iceland Lichtenstein)?	☒ Yes - Both suppliers uses Microsoft Azure Data Centres to store and process data, with both (UK South and UK West) in the UK. ☐ No
If 'No' to the previous question, does the country in which it is being hosted have adequate protection for the rights and freedoms of data subjects, as defined by the European Commission?	☐ Yes ☐ No ☒ N/A
Is the Cloud service provider hosted on N3 or the internet?	☒ Yes - The data is hosted via the internet and can be accessed on the N3 network. ☐ No
What happens to the data in the event of the Cloud provider's business closure / insolvency?	Data shall be destroyed in line with the appropriate industry security standard as provided by appropriate governing body as updated from time to time.
What arrangements would there be in place at the end of the contract with the Cloud service provider to transfer the data? Would there be any associated costs incurred by the Trust?	The agreement provides for the transfer of data at no additional cost.
Who would legally own any data uploaded to the Cloud application by the Trust or its staff?	Joint Controllers between GP + LA + NHS Trust in St Helens – See Schedule 1 of the data sharing agreement
Does the provider have other NHS contracts, and have you spoken to these organisations as part of due diligence? Please give full details.	☒ Yes – System C and Graphnet are widely in used by other NHS organisation. Both suppliers already provide various services to the Trust. ☐ No

What security frameworks and policies are in place by the Cloud service provider? Please direct the reviewer to them online, or embed copies here.	See supplier’s due diligence questionnaire.
What safeguards does the Cloud service provider have in place / offer to protect against Cyber Security attacks? Please direct the reviewer to documents online, or embed copies here.	As per above
Will the transit of data between the Trust and the Cloud service provider be secure, e.g. by use of https?	Graphnet – Data are transferred securely via SFTP and HTTPS with Transport Layer Security (TLS) 1.2 (or later), which is an industry standard protocol, with 2,048-bit RSA/SHA256 encryption keys, as recommended by CESG/NCSC. System C - Data are transferred using “secure protocols”, such as HTTPS and TLS 1.2.

8: Business Continuity

Do you have a Business Continuity Plan in place if the system and / or process fails or is unavailable for any reason? If yes, please embed the business continuity document in this box or provide a link:	☐ Yes ☒ No In the event that the Shared care record was unavailable to health and social care teams, staff will revert to traditional methods of obtaining information via telephone and Secure emails.

9: Additional Comments

Do you wish to supply additional comments about the system / asset? If yes, please input comments in the box:	☐ Yes ☒ No Please enter text here:

11: Approval of Legal Basis Identified by the DPO

Article 6(1) – Legal Basis for processing personal data	
(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.	☐
(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.	☐
(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).	☐
(d) Vital interests: the processing is necessary to protect someone's life.	☐
(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.	☒
(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)	☐

Article 9(2) Legal basis for processing sensitive special category data	
(a) Explicit consent	☐
(b) Obligations under employment	☐
(c) Vital interests	☐
(d) For political, philosophical, religious or trade union aim provided	☐
(e) Personal data manifestly made public by data subject	☐
(f) Necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity	☐
(g) Necessary for reasons of substantial public interest on the basis of EU or Member State law	☐
(h) Preventative or occupational medicine for assessing the working capacity of an employee, medical diagnosis, provision of health or social care, treatment/ management of health or social care systems and services on the basis of EU or member state law or a contract with a health professional	☒
(i) Public interest in the area of public health	☐
(j) Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes	☐

12: Risk Assessment

Reassess and accept the risks

Please insert rows below if there are more than three risks identified.

Privacy risk	Control	Likelihood after control	Impact after control	Risk Accepted by
Inappropriate access by unauthorised person/s	- Role based access controls - Internal audit/logs - Supplier Contracts - Policies - Restricted access arrangements in place for supplier - Training - Internal SOP's - Leavers process - Inactive users process	☐- 1 Rare ☒ - 2 Unlikely ☐ - 3 Possible ☐ - 4 Likely ☐ - 5 Almost Certain	☐- 1 No Harm ☒ - 2 Low Harm ☐- 3 Moderate ☐ - 4 Major Harm ☐ - 5 Catastrophic	Risk accepted at a score of 4 by the Group
Accuracy/ Quality of the Data	- Quality assurance checks - KPI's - Data Quality groups in place - Policies - Housekeeping - Review of duplicate records - Training	☐- 1 Rare ☒ - 2 Unlikely ☐ - 3 Possible ☐ - 4 Likely ☐ - 5 Almost Certain	☐- 1 No Harm ☒ - 2 Low Harm ☐- 3 Moderate ☐ - 4 Major Harm ☐ - 5 Catastrophic	Risk accepted at a score of 4 by the Group
Deliberate alteration of records	- Role based access controls - Internal audit/logs - Contracts - Policies - Disciplinary process - Restricted access arrangements in place for supplier - Training - Internal SOP's - Back up process to recover records	☐- 1 Rare ☒ - 2 Unlikely ☐ - 3 Possible ☐ - 4 Likely ☐ - 5 Almost Certain	☐- 1 No Harm ☒ - 2 Low Harm ☐- 3 Moderate ☐ - 4 Major Harm ☐ - 5 Catastrophic	Risk accepted at a score of 4 by the Group
Malicious Data loss	Policies - Role based access	☐- 1 Rare ☐ - 2 Unlikely	☐- 1 No Harm ☐ - 2 Low Harm	Risk accepted at a score of 9 by the Group

	- Local Audit procedures - Training - Back up recovery - Resilience plan	☒ - 3 Possible ☐ - 4 Likely ☐ - 5 Almost Certain	☒- 3 Moderate ☐ - 4 Major Harm ☐ - 5 Catastrophic	
Loss of connection	Resilient Infrastructure - Supplier contracts - SLA’s - BCP’s in place	☐- 1 Rare ☒ - 2 Unlikely ☐ - 3 Possible ☐ - 4 Likely ☐ - 5 Almost Certain	☐- 1 No Harm ☒ - 2 Low Harm ☐- 3 Moderate ☐ - 4 Major Harm ☐ - 5 Catastrophic	Risk accepted at a score of 4 by the Group
CoIN security	- Escalation to suppliers - Regional Cyber Group - Supplier controls - Pen Testing	☐- 1 Rare ☐ - 2 Unlikely ☒ - 3 Possible ☐ - 4 Likely ☐ - 5 Almost Certain	☐- 1 No Harm ☒ - 2 Low Harm ☐- 3 Moderate ☐ - 4 Major Harm ☐ - 5 Catastrophic	Risk accepted at a score of 6 by the Group
Cyber Attack	CareCerts - Patching locally - Patching /Supplier - Firewalls - BCP - Anti-malware - Backup recovery - Regional Cyber Group	☐- 1 Rare ☐ - 2 Unlikely ☒ - 3 Possible ☐ - 4 Likely ☐ - 5 Almost Certain	☐- 1 No Harm ☐ - 2 Low Harm ☒- 3 Moderate ☐ - 4 Major Harm ☐ - 5 Catastrophic	Risk accepted at a score of 9 by the Group

Please provide any comments for mitigation here:

Graphnet hold the ISO 27001 and Cyber Essentials Plus accreditations and is working towards ISO 27018. The company and applications are compliant with these standards and is tested annually for them. The company also completes the Data Security and Protection Toolkit annually.

13: Information Governance Review

The IG team is required to review all DPIAs before seeking necessary approval.

First Review

First review completed by:	**Shola Adodo**
Job title	**Senior Information Governance Officer**
Date of review	
Recommendation	**Further Questions require answers**

Second Review

Second review completed by:	
Job title	
Date of review	
Recommendation	

14: Approval and Sign off

Signatures

Information Security (For applications involving the use of Cloud technology)

Name:	Richard Priest
Title:	Network and IT Security Manager
Email:	
Signature & Date	30/04/2021

Data Protection Officer

Name:	Camilla Bhondoo
Title:	Head of Risk Assurance & Data Protection Officer
Email:	
Signature & Date	30/04/2021
Recommendations to SIRO and forward actions following DPIA approval:	Recommend SIRO to approve. Agree with Risk Scores. Recommendations: Participating organisations: Ensure this processing is on each participating's Information Asset Register and that this is reviewed at least annually to check whether the processing is still relevant, legal basis is still correct etc. This will also prompt a review to who has access and check this is the correct

	level of access. Reminder that participating organisations feeding into the Care Record must ensure they apply their Data Quality process / procedure. Organisations will be reliant on data being up to date, accurate and relevant. Review Privacy Notices and Communications to ensure they are up to date on a regular basis. Any changes to this processing – this DPIA must be revisited and updated. Where data subjects exercise their individual rights (i.e. Subject access, right to erasure etc) they will be advised to contact each organisation feeding into the Care Record, each organisation must process as per their policy.

Senior Information Risk Owner

Name:	Christine Walters
Title:	Director of Informatics
Signature & Date	30th April 2021

Glossary of Terms

Item
Definition

Personal Data

This means data which relates to a living individual which can beidentified:
A) from those data, or
B) from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller.

It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

Special Category Data This means personal data consisting of information as to the:

A) racial or ethnic group of the individual
B) the political opinions of the individual
C) the religious beliefs or other beliefs of a similar nature of the individual
D) whether the individual is a member of a trade union
E) physical or mental health of the individual
F) sexual life of the individual
G) the commission or alleged commission by the individual of any offence
H) any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings

Direct Marketing This is "junk mail" which is directed to particular individuals. The mail which are addressed to "the occupier" is not directed to an individual and is therefore not direct marketing.

Direct marketing also includes all other means by which an individual may be contacted directly such as emails and text messages which you have asked to be sent to you.

Direct marketing does not just refer to selling products or services to individuals, it also includes promoting particular views or campaigns such as those of a political party or charity.