




## Share2Care Data Protection Impact Assessment (DPIA)



Data Protection Act  
2018

---

<b>Date form started:</b>	3.12.19
<b>By Whom:</b>	
<b>DPO approved:</b>	4.12.19
<b>IT Security approved:</b>	5.12.19
<b>SIRO approved:</b>	5.12.19
<b>Submitted to ICO Y/N:</b>	No

Information Reader Box	
Document Purpose:	Ensure consistent application of DPIA process in programme
Document Name:	Data Protection Impact Assessments
Author:	<div>██████████ – Share2Care Programme Manager</div> <div>██████████ –LPRES IG Support</div>
Document Origin:	NECS Standard Operating Procedure - Information Governance: <i>Data Protection Impact Assessments</i> (Privacy by Design) (2018)
Target Audience:	Share2Care Partner Organisations
Description	Template Share2Care Data Protection Impact Assessment with Guidance
Cross Reference:	<i>DPIAs are applicable to all other procedures, policies, and SOPs</i>
Superseded Document:	N/A
Action Required:	To complete and sign as appropriate for your organisation
Contact Details (for further information and feedback)	Name: Share2Care Admin  E-mail: <a href="mailto:Share2Care@alderhey.nhs.uk">Share2Care@alderhey.nhs.uk</a>
Document Status	
<p>This is a controlled document. Whilst this document may be printed, the electronic version available on the shared Microsoft Any printed copies of this document are not controlled.</p> <p>As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.</p>	

## Contents

Background and Guidance .....	4
Introduction .....	4
Overview of Share2Care DPIA.....	4
Roles and Responsibilities .....	5
DATA PROTECTION IMPACT ASSESSMENT .....	6
<b>Share2Care/e-Xchange Programme</b> .....	6
Information Flows: .....	6
Information Flow Functional Description .....	6
Categories of Personal Data to be Processed: .....	8
Consent Process and Right to Object (Opt-out) .....	9
Data Protection Review .....	10
Data Processors.....	11
Action Plan .....	14
Risk Assessment.....	14
DPIA Summary .....	15
Signature Page .....	16
Appendix 1 – Share2Care Screening Tool.....	17
Appendix 2 – Share2Care Data Sharing Agreement.....	17

## Background and Guidance

### Introduction

- a. Share2Care is a collaborative programme between Cheshire and Merseyside and the Lancashire & South Cumbria Health and Care Partnerships to deliver the electronic sharing of health and care records.
- b. Through the Share2Care programme, the Connect/e-Xchange workstream, will both connect and support the integration of our local health and care organisations. The workstream will ensure that information is available to the right people, in the right place, at the right time to deliver and drive service delivery, integration and transformation.
- c. Share2Care will augment, improve, and support the transformational journey. The programme will drive adoption of digital services and make accessibility to real-time shared information the 'norm'. The programme will seek large-scale collaborative solutions to address system-wide challenges, including:
  - i. Making organisational care data "boundary-less", supporting patient care regardless of setting
  - ii. Providing patients with seamless access to their care record
  - iii. Supporting complex care needs delivered across super-regional / tertiary centres
- d. The solution is known as e-Xchange. The e-Xchange solution will give providers of health and care access to the information which is necessary, proportionate and relevant to their role.

### Overview of Share2Care DPIA

- e. Article 35(1) of the General Data Protection Regulations says that you must do a DPIA where a type of processing is likely to result in a high risk to the rights and freedoms of individuals.
- f. A Data Protection Impact Assessment (DPIA) is a process which can help an organisation identify the most effective way to comply with its data protection obligations. In addition, DPIAs will allow organisations to meet individuals' expectations of privacy.
- g. An effective DPIA will facilitate the identification and minimisation of potential data protection risks at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

- h. In February 2014, the Information Commissioner issued a code of practice under Section 51 of the Data Protection Act (DPA) in pursuance of the duty to promote good practice. The DPA says good practice includes, but is not limited to, compliance with the requirements of the Act and undertaking a DPIA ensures that a new project is compliant.
- i. One of the new requirements of the GDPR that came into force in May 2018 is an obligation to conduct a DPIA before carrying out types of processing likely to result in high risk to individual's interests
- j. The following document is the Share2Care DPIA template which your organisation can use to commence or update your sharing relationship with the Share2Care programme.
- k. If your organisation already has a standard DPIA template, the appendix lists a **DPIA Screening Tool** which should assist in completing your local DPIA.

## Roles and Responsibilities

- l. **Executive Sponsor:** The owner of any data protection risks identified within the DPIA. This person is an appropriately senior manager, ideally a member of the Executive Team, assigned to the relevant Directorate.
- m. **Data controller:** exercises control over the processing and carries data protection responsibility. Their activities will include significant decision making.
- n. **Data processor:** simply processes data on behalf of a data controller and their activities are more limited to 'technical' aspects
- o. **Sub processor:** Under GDPR, the controller must give its prior written authorisation when its processor intends to entrust all or part of the tasks assigned to it to a sub processor. The Process remains fully liable to the controller for the performance of the sub-processor's obligations.

## DATA PROTECTION IMPACT ASSESSMENT

<b>Version:</b>	V1	
<b>Reference No:</b>		
<b>Sharing Initiative Name:</b>	Share2Care/e-Xchange Programme	
<b>Sharing Start Date:</b>	3.12.19	
<b>Lead Organisation(s):</b>	Alder Hey	
<b>Workstream Lead</b>	<b>Name</b>	Jim Hughes
	<b>Designation</b>	Strategic Advisor Digital Programme
	<b>Telephone</b>	0151 473 2786
	<b>Email</b>	Jim.Hughes@Merseycare.nhs.uk
<b>DPO Review</b>	<b>Name</b>	Linda Yell
	<b>Designation</b>	Head of Information Governance/DPO
	<b>Telephone</b>	0151 471 2686
	<b>Email</b>	Linda.Yell@Merseycare.nhs.uk
	<b>Date of review</b>	4.12.19
<b>Designated Officer Approval</b>	<b>Name</b>	Asim Patel
	<b>Designation</b>	CIO
	<b>Telephone</b>	01925 664066
	<b>Email</b>	Asim.Patel@Merseycare.nhs.uk
	<b>Date of review</b>	5.12.19

## Information Flows:

Risks associated with the information flows can be assessed and where necessary mitigated. Any changes to information flows throughout the project will prompt a review of the privacy risks as they may change.

### Information Flow Functional Description

Information Flow Type	Direct Care
Description of information flow	Participating sites publish approved clinical information, which is displayed to health and social care professionals for direct care.
Source of information	Aintree University Hospital NHS Foundation Trust; Alder Hey Children's NHS Foundation Trust; Bridgewater Community Healthcare NHS Foundation Trust; Cheshire and Wirral Partnership NHS Foundation Trust; The Clatterbridge Cancer Centre NHS Foundation

	Trust; Countess of Chester Hospital NHS Foundation Trust; East Cheshire NHS Trust; Liverpool Heart and Chest NHS Foundation Trust; Liverpool Women's NHS Foundation Trust; Mersey Care NHS Foundation Trust; The Mid Cheshire Hospitals NHS Foundation Trust; NW Boroughs Partnership NHS Foundation Trust; Royal Liverpool and Broadgreen University Hospitals NHS Trust ; St Helens and Knowsley Teaching Hospitals NHS Trust; Southport and Ormskirk Hospital NHS Trust ; The Walton Centre NHS Foundation Trust; Warrington and Halton Hospitals NHS Foundation Trust; Wirral Community NHS Foundation Trust; Wirral University Teaching Hospital NHS Foundation Trust; Lancashire Teaching Hospitals Foundation Trust; Blackpool Teaching Hospitals NHS Foundation Trust; University Hospitals of Morecambe Bay NHS Foundation Trust; Cumbria Partnership NHS Foundation Trust; East Lancashire Hospitals NHS Trust; Lancashire Care NHS Foundation Trust; North West Ambulance Service; Cheshire East Council; Cheshire West and Chester Council; Halton Borough Council; Knowsley Borough Council; Liverpool City Council; Sefton Council; St Helens Council; Warrington Borough Council; Wirral Council; Lancashire County Council; Blackpool Council ; Blackburn with Darwen; Cumbria County Council; Lancaster Council; NHS Blackburn and Darwen CCG; NHS Chorley and South Ribble CCG; NHS East Lancashire CCG; NHS Eastern Cheshire CCG; NHS Greater Preston CCG; NHS Halton CCG; NHS Knowsley CCG; NHS Liverpool CCG; NHS Sefton CCG; NHS South Cheshire CCG; NHS Southport and Formby CCG; NHS St Helen CCG; NHS The Bay CCG (formerly Morecambe Bay); NHS Vale Royal CCG; NHS Warrington CCG; NHS West Cheshire CCG; NHS Wirral CCG
Method of transfer/transmission	Published information is viewed, not transmitted. Information stored in originating Trust server. Information for retrieval is sent to ForConnect (Phillips/Forcare), which is held in local servers seated within the Trust network domain. A link to published data is registered in the central registry. When an authorised user accesses the system, a link is routed to the document held in the servers of the respective sites, and a view of that document is displayed to the user.
Destination of information	Remains in source system.
Persistent or temporary (if persistent, detail the storage location following transfer)	Temporary.
No. of records/individuals affected	4.3 million individuals across Cheshire, Merseyside, Lancashire and South Cumbria.
Deletion of information	Information can only be deleted by the source organisation.

Risks/actions identified	None identified as no persisted transmission of patient information.
--------------------------	--

### Categories of Personal Data to be Processed:


<b>Data Processed</b>	<ul style="list-style-type: none"> <li>• Name, Address (home or business), Postcode</li> <li>• NHS Number</li> <li>• Date of Birth</li> <li>• Online identifier (e.g. Email Address, IP Address)</li> <li>• Identification Number (e.g. Payroll Number, Passport Number, Driving Licence Number, National Insurance number)</li> <li>• Location Data</li> <li>• Racial/Ethnic Origin</li> <li>• Adoption</li> <li>• Religious or Philosophical Beliefs</li> <li>• Employment, School</li> <li>• Genetic Data</li> <li>• Biometric Data (e.g. Fingerprints)</li> <li>• Safeguarding</li> <li>• Health (health data includes) <ul style="list-style-type: none"> <li>• clinical diagnosis and history,</li> <li>• treatment plans,</li> <li>• medications,</li> <li>• discharge summaries,</li> <li>• clinic letters,</li> <li>• radiology data,</li> <li>• laboratory data,</li> <li>• and any other pertinent health data for direct patient care.</li> </ul> </li> <li>• Social Care</li> <li>• Sexual Life</li> <li>• Sexual Orientation</li> </ul>
<b>Lawful Basis:</b>	<ul style="list-style-type: none"> <li>• Legal Duty</li> <li>• Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller</li> <li>• Necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care, or treatment or the management of health or social care systems and service</li> </ul>



## Consent Process and Right to Object (Opt-out)

Consent is not a requirement for direct care and is not a relevant lawful basis for this system.

However, the right to object under §21 of the General Data Protection Regulation 2016, as enacted, is relevant. Patients and service users have a right to object to their medical information being used and can register this objection in writing, or verbally to the clinician concerned.

<b>GDPR Lawful Bases</b>	<p>The General Data Protection Regulations (GDPR) makes the following provisions for processing personal data in relation to this project:</p> <ul style="list-style-type: none"> <li>• The GDPR lawful basis for 'processing of personal data' is permitted under 'Article 6(1)(e) – official authority'</li> <li>• The GDPR lawful basis for 'processing of special category data' is permitted under 'Article 9(2)(h) – provision of health'</li> </ul>
<b>The right to object under GDPR</b>	<p>Patient opt-out is with the data controller that stores the information viewed in e-Xchange, e.g., the GP Practice or Trust where the data originates. The Share2Care Data Sharing Agreement informs organisations of tools they can use to inform individuals of their rights to object.</p>
<b>Direct Care</b>	<p>The Cheshire and Merseyside Clinical Implementation Advisory Group endorsed recommendation that Consent is not required as lawful basis of viewing record for direct clinical care. <i>Local Health and Care Records Guidance on Meeting the Duty of Transparency</i> states: "Explicit consent is not required when confidential patient information (personally identifiable information) is being processed for individual care purposes and should not be sought. The use of data for individual care purposes should rely upon implied consent or the patient's reasonable expectations as a lawful basis. As the sharing of health and care records becomes more commonplace across the country patients increasingly expect that this will be the case."</p> <div data-bbox="673 1783 738 1845" data-label="Image">  </div> <p>Local Health and Care Records_ Guidai</p>

## Data Protection Review



A review of the Principles relating to the processing of personal data under the GDPR should be undertaken to ensure projects take account of these and employ a 'privacy by design' approach.

Principle		Compliance	
Lawfulness, fairness and transparency	Lawful Basis	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.	
		The Health and Social Care (Safety and Quality) Act 2015 inserted a legal Duty to Share Information In Part 9 of the Health and Social Care Act 2012 (health and adult social care services: information)	
		Official authority:	
		GP Practices	NHS England's powers to commission health services under the NHS Act 2006. Also, Article 6 (1) c for GPs when subject to statutory regulation
		NHS Trusts	National Health Service and Community Care Act 1990
	NHS Foundation Trusts	Health and Social Care (Community Health and Standards) Act 2003	
	Local Authorities	Local Government Act 1974 Localism Act 2011 Children Act 1989 Children Act 2004 Care Act 2014	
	Fairness	Individuals can exercise the following rights with respect to their data, where applicable, by contacting the source organisation of their data: <ul style="list-style-type: none"><li>• Right of access</li><li>• Right to rectification</li><li>• Right to erasure</li><li>• Right to restrict processing</li><li>• Right to data portability</li><li>• Right to object</li><li>• Rights related to automated decision making including profiling</li></ul>	

	Transparency	<p>The responsibility for transparency lies firmly with the controllers who are the partner organisations within Share2Care.</p> <p>A transparency notice from Share2Care can be found on the Share2Care website: <a href="http://www.share2care.nhs.uk">www.share2care.nhs.uk</a></p>
Purpose limitation		Share2Care e-Xchange is for the purposes of direct care only.
Data minimisation		<p>Sensitive data excluded from retrieval follows the recommendations made by The Royal College of General Practitioners (RCGP) ethics committee and the Joint GP IT Committee:</p> <ul style="list-style-type: none"> <li>• Gender reassignment.</li> <li>• Assisted conception and in vitro fertilisation (IVF)</li> <li>• Sexually transmitted diseases (STD)</li> <li>• Termination of pregnancy</li> </ul>
Accuracy		Incident management process related to incorrect documentation is in place with Share2Care and Informatics Merseyside. Where a document is discovered that is incorrect, the Trust identifying the document will log within local incident management systems, notify IT, and IT will notify the 3 <sup>rd</sup> Line support of Informatics Merseyside to notify the originating Trust.
Storage limitation		NA – no data is stored.
Integrity and confidentiality		Access levels to information available through e-Xchange will be based upon the role held by the provider of health and care. Information will be shared which is necessary, relevant and proportionate to the role the individual fulfils.

## Data Processors

Where data processors are to be used, a legally binding contract (Information Processing Agreement) must be in place which includes the necessary contractual elements required under the GDPR. An assessment of the data processor's ability to comply with its terms should also be conducted (due diligence).

Contract criterion	Contract Location
Processor is to act only on instruction of Controller	Informatics Merseyside Aimes.
<p>Agreed security standards such as IGT or ISO 27000</p>	<p>Phillips/Forcare is ISO27001 certified since 2016 and has a certification for NEN7510 as well. NEN7510 is a Dutch standard about information security for healthcare professionals.</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  <p>ISO 27001 certificate.pdf</p> </div> <div style="text-align: center;">  <p>ISO 13485 certificate.pdf</p> </div> </div>
<p>Incident management is included and the requirement to immediately report</p>	<p><b>Forcare Incident Management:</b></p> <p>A dedicated information security incident management process exists besides the regular incident management process which includes data breaches.</p> <p>A dedicated Information Security incident management policy exists for Share2Care.</p> <p>Users are trained to recognise security incidents and methods for reporting them. These incidents are reported directly to the Security Officer (in case of absence it is reported to the COO or reporting to Philips Security Officer is also a possibility).</p> <p>The Security Officer will register, monitor and sometimes coordinate the incident response, together with COO. The COO will communicate to the responsible person within the partner organisation.</p> <p>Upon incident closure, a root cause analysis takes place on each incident, and this evaluation is reported to the</p>

	partner organisations Senior Management Team by the Forcare Security Officer.
Record retention is detailed both during and after the agreement	N/A – no data is persisted or retained. Information is held within the Partner Organisations local server, and subject to local record retention policies.
Actions to be taken for FOI and EIR are included	N/A - FOI and EIR should be undertaken with the Partner Organisation that holds the data. Share2Care e-Xchange does not persist data.
Training is a requirement for all staff of the processor handling the data	Phillips/Forcare will provide the Trusts with train the trainer and training material, all users should be trained to make safe use of the platform. Further training support can be found on the <a href="http://www.s2chelp.nhs.uk">www.s2chelp.nhs.uk</a> page.
All staff are held under a confidentiality agreement in staff contracts	<p>Yes. All staff accessing Share2Care has a duty of confidentiality. All partner organisations would have signed up to the Data Sharing Agreement which states:</p> <p>“All signatories to this agreement are required to ensure they fulfill their obligations under the General Data Protection Regulation and Data Protection Act 2018 and the Common Law Duty of Confidentiality.”</p> <p>Additionally, all staff involved in direct care would be subject to the Data Protection Act 2018 and the Caldicott Principles.</p>

## Action Plan

*Any actions arising from the DPIA should be detailed here.*

Actions are prioritised into those which are considered essential to ensure the success of the project (Required) and those which are recommended to support the success of the project (Recommended). The source of the requirement is also recorded as follows:

- Legal Requirement – The action must be completed to ensure compliance with the law;
- Assurance – The action will provide assurance to stakeholders and/or provide evidence that best practice is being followed/adopted;
- Best Practice – The action is considered best practice and so any deviation from this should be explicitly justified;
- Operational – The action is considered necessary to ensure operational success.

Action	Priority	Requirement	Accepted by project and added to the action plan	Comments

## Risk Assessment

Risks identified by the DPIA should be assessed using the following model and documented within the DPIA Summary. Identified risks with Share2Care e-Xchange can be found in the below attached hazard log:



Share2Care  
e-Xchange Hazard log

## Risk Matrix

		Impact				
		Trivial	Minor	Moderate	Major	Extreme
Probability	Rare	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very Likely	Medium	Medium	High	High	High

## DPIA Summary

Project Name:	Share2Care/e-Xchange		
Lead Organisation(s):			
Project Summary:	Share2Care e-Xchange platform provides read-only access to clinical information for healthcare professionals and patients across all healthcare settings (primary care, secondary care and social care) across the UK North West Coast geographical boundary. The platform is able to share this read-only data by using the international IHE (Integrating the Healthcare Enterprise) standards, and is aligned to the NHS Digital strategies for interoperability in healthcare in the UK. The e-Xchange solution has a central XDS component housed in the iMerseyside data centre and local components within the partner organisation		
Stakeholders	Aintree University Hospital NHS Foundation Trust; Alder Hey Children's NHS Foundation Trust; Bridgewater Community Healthcare NHS Foundation Trust; Cheshire and Wirral Partnership NHS Foundation Trust; The Clatterbridge Cancer Centre NHS Foundation Trust; Countess of Chester Hospital NHS Foundation Trust; East Cheshire NHS Trust; Liverpool Heart and Chest NHS Foundation Trust; Liverpool Women's NHS Foundation Trust; Mersey Care NHS Foundation Trust; The Mid Cheshire Hospitals NHS Foundation Trust; NW Boroughs Partnership NHS Foundation Trust; Royal Liverpool and Broadgreen University Hospitals NHS Trust ; St Helens and Knowsley Teaching Hospitals NHS Trust; Southport and Ormskirk Hospital NHS Trust ; The Walton Centre NHS Foundation Trust; Warrington and Halton Hospitals NHS Foundation Trust; Wirral Community NHS Foundation Trust; Wirral University Teaching Hospital NHS Foundation Trust; Lancashire Teaching Hospitals Foundation Trust; Blackpool Teaching Hospitals NHS Foundation Trust; University Hospitals of Morecambe Bay NHS Foundation Trust; Cumbria Partnership NHS Foundation Trust; East Lancashire Hospitals NHS Trust; Lancashire Care NHS Foundation Trust; North West Ambulance Service; Cheshire East Council; Cheshire West and Chester Council; Halton Borough Council; Knowsley Borough Council; Liverpool City Council; Sefton Council; St Helens Council; Warrington Borough Council; Wirral Council; Lancashire County Council; Blackpool Council ; Blackburn with Darwen; Cumbria County Council; Lancaster Council; NHS Blackburn and Darwen CCG; NHS Chorley and South Ribble CCG; NHS East Lancashire CCG; NHS Eastern Cheshire CCG; NHS Greater Preston CCG; NHS Halton CCG; NHS Knowsley CCG; NHS Liverpool CCG; NHS Sefton CCG; NHS South Cheshire CCG; NHS Southport and Formby CCG; NHS St Helen CCG; NHS The Bay CCG (formerly Morecambe Bay); NHS Vale Royal CCG; NHS Warrington CCG; NHS West Cheshire CCG; NHS Wirral CCG		
Privacy Risks Identified	Controls	Result	Evaluation
Other recommendations:			

## Signature Page

Data Protection Officer Sign Off	
Name	[REDACTED]
Job Title	Head of Information Governance/DPO
Organisation	Mersey Care NHS Foundation Trust
Signature	[REDACTED]
Date of signing	4.12.19

Designated Officer Sign Off	
Name	[REDACTED]
Job Title	Chief Information Officer
Organisation	Mersey Care NHS Foundation Trust
Signature	[REDACTED]
Date of signing	5.12.19



## Appendix 1 – Share2Care Screening Tool

If a local DPIA is to be completed, please use the **DPIA Screening Tool** which should assist in completion. This can be sent via email with the subject **IG** to [share2care@alderhey.nhs.uk](mailto:share2care@alderhey.nhs.uk)



Share2Care DPIA  
Screening Tool.docx

## Appendix 2 – Share2Care Data Sharing Agreement

Please see attached copy of the Share2Care Data Sharing Agreement to be signed off by your organisations Caldicott Guardian:



Share2Care\_Sharing  
Agreement\_v2\_2019.