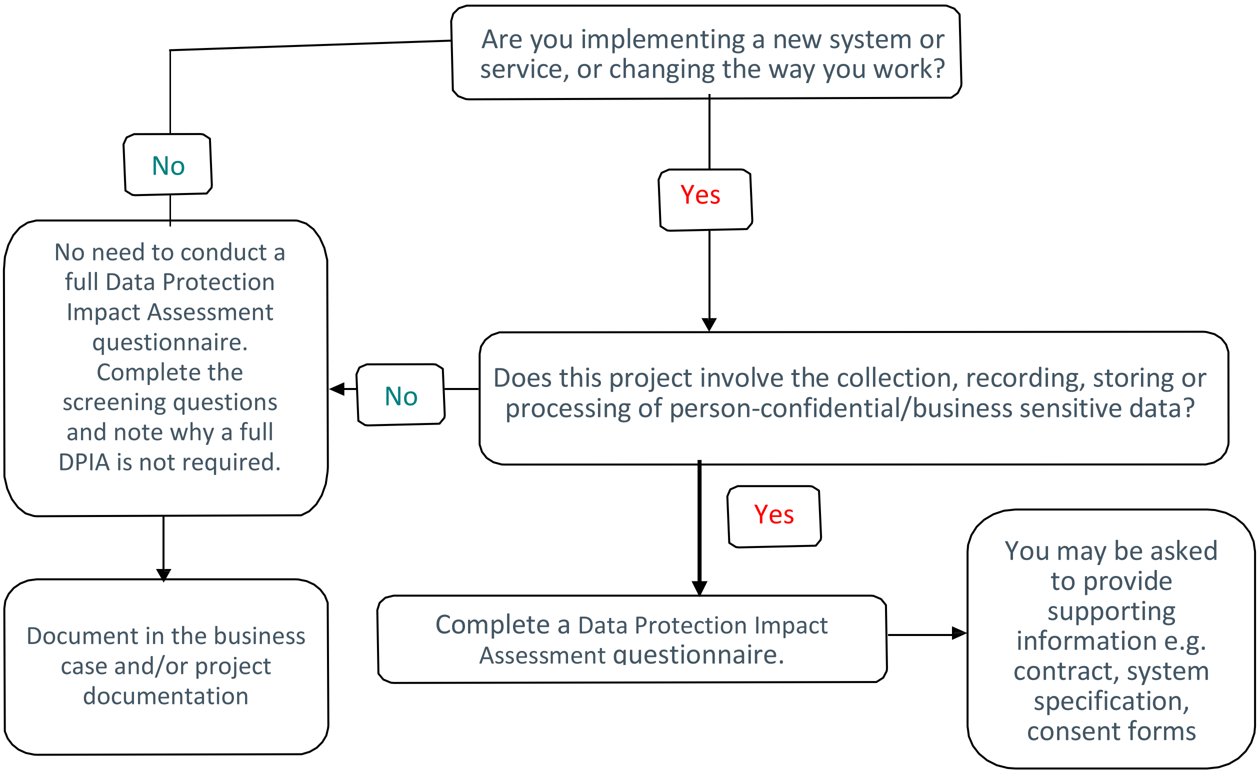
Do I Need to Complete a Data Protection Impact Assessment questionnaire?



Are you implementing a new system or service, or changing the way you work?

No

No need to conduct a full Data Protection Impact Assessment questionnaire. Complete the screening questions and note why a full DPIA is not required.

Document in the business case and/or project documentation

Yes

Does this project involve the collection, recording, storing or processing of person-confidential/business sensitive data?

No

Yes

Complete a Data Protection Impact Assessment questionnaire.

You may be asked to provide supporting information e.g. contract, system specification, consent forms

When deciding whether a DPIA questionnaire is required, if the first answer is ‘yes’, but the second response is ‘unsure’, please complete the questions in section 1 of the DPIA questionnaire to assist the decision. Further guidance can be sought from the Information Governance Team: nelcsu.Information-Governance@nhs.net.

It is a requirement of the General Data Protection Regulations that all systems have a DPIA conducted, including any systems processing data that do not require a full DPIA, i.e. you must complete at least the screening questions and identify why a full DPIA is not required.

If you are assessing a system and it does not have a DPIA, including one that identifies that a full DPIA is not required, please complete the relevant section of this questionnaire.

The questionnaire will be reviewed by the stakeholders, including the IG Lead and the recommendation from the questionnaire will be notified to the Director (Information Asset Owner). The recommendation will be either:

1. A full DPIA is required where the new process or change of use of PCD/Business Sensitive data requires more thorough investigation.
2. The DPIA questionnaire will be signed off by the Information Asset Owner/SIRO and the DPIA log updated by the IG Lead.

There is an Information Security Procurement Questionnaire (for use in the commissioning process for new information systems), an Information Risk Questionnaire template and an ICT System Security Risk Assessment available to assist in assessing the risks.

Background		
Work Stream	Transferring Care Home Resident Information into Health	
Work Stream Lead	Name	Viccie Nelson
	Designation	Senior Transformation Manager
	Telephone	07833046785
	Email	Viccie.nelson@swlondon.nhs.uk
Information Asset Owner (if different from above)		Belmont House Care Home, Information Asset Owner: Arthur Tanare, Care Home Manager Grasmere Rest Home, Information Asset Owner: Moyra Hillman, Care Home Manager
Implementation Date		31st January 2019

Key Information – Please be as comprehensive as possible	
Project Name	Digitalising the Red Bag Paperwork in Sutton, Phase 1
Description of Project	In Sutton, there is a well-established Red Bag scheme (called the Hospital Transfer Pathway) which involves residents of care homes taking a Red Bag with them when they need to go hospital urgently or in an emergency. The Red Bag that goes with the resident contains:

- Paperwork (copies of This Is Me, Older Person's Assessment Form (baseline assessment), CARES Escalation Record, Advance Care Plan, DNAR, and MAR sheet/s)
- Medications
- Clothes to return home in
- Toiletries
- Personal belongings, such as, glasses, hearing aids etc

This project is about digitalising the Red Bag paperwork so that a digital copy goes directly from the care home to the hospital at the time when the resident is physically transferred.

Two Care Homes will participate in this pilot project: Belmont House and Grasmere Rest Home, sharing information with Epsom and St Helier University Hospitals NHS Trust (ESH Trust).

Belmont House uses Person Centred Software's (PCS) digital platform Mobile Care Monitoring (MCM). This system is also used more widely in care homes across the South West London Health and Care Partnership and nationally. This mobile care monitoring system supports the production of a hospital pack to generate information to be included in the Red Bag. The hospital pack includes the This is Me document and baseline observations and clinical data (such as, BP, pulse, temperature), symptoms and other social and medical information (such as, allergies). At present the hospital pack is printed and physically sent with the care home resident to the hospital when urgent/emergency care is required.

This project seeks to digitise this process, whereby an electronic version of the hospital pack is transferred directly to the hospital from the care home, from within MCM. This digitised hospital pack will be sent via a secure method of transfer, to the e-documents tab on the ESH Trust's electronic patient record system.

Since Belmont House already uses the MCM software, this process is a relatively simple change to the home's current processes. The change is to add further information, such as the resident's medication administration record, to MCM which will then be added in to the digital hospital pack.

In the second care home, Grasmere Rest Home, paper records only are used. This project seeks to transfer a digital copy of the Red Bag paperwork via a secure transfer to the ESH record as described above. The project will do this through the care home having access to the MCM software online and having a mobile device which supports uploading documents via photography. Once the documents are in the software the care staff can use the mobile device to provide automated transfer to the hospital.

Once the secure transfer is successful to ESH Trust then the plan is to work out how to:

- transfer to the London Health Information Exchange (HIE) record
- combine with online access to coordinate my care software

	- send a digital copy of the discharge summary directly to the care home. Both Care Homes will be supported through the DSP Toolkit to reach 'Standards Met' level, and to have NHS.net email in place. By extending the existing hospital pack information and developing MCM to be able to transfer the Red Bag electronically using automated transfer (or NHS mail if a back-up is required) rather than just relying on printed off required information, there would be significant benefits for the care home resident as well as staff in the care home and in ESH Trust. The sharing of the data between the care homes and ESH Trust will continue to be on an ad-hoc basis for this trial.

Key Contacts	
Key Stakeholders Names & Roles	Belmont House Care Home Manager: Arthur Tanare Grasmere Rest Home Care Home Manager: Moyra Hillman Person Centred Software Ltd Co-Founder and Director: Simon Papworth Epsom and St Helier University Hospitals NHS Trust IG Manager and DPO: Paul Kenny
Date	19th November 2018

Screening Questions	Yes or No
Will the project involve the collection of information about individuals?	Yes
Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business?	No
Will the project compel individuals to provide information about themselves?	Yes
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	No
Are you using information about individuals for a new purpose or in a new way that is different from any existing use?	No
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of data to make a decision about care that's automated.	Yes
Will the project result in you making decisions about individuals in ways which may have a significant impact on them? e.g. service planning, commissioning of new services	No
Will the project result in you making decisions about individuals in ways which may have a significant impact on identifiable individuals? i.e. does the project change the delivery of direct care. **N.B.** If the project is using anonymised/pseudonymised data **only**, the response to this question is "**No**".	No
Will the project require you to contact individuals in ways which they may find intrusive?	No
Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners?	Yes
Does the project involve new or significantly changed handling of a considerable amount of personal and/or business sensitive data about each individual in a database?	Yes
Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal and/or business sensitive data from multiple sources?	Yes

If any of the screening questions have been answered "YES", then please continue with the Data Protection Impact Assessment Questionnaire (below).

If all questions are "NO", please return the document to the Information Governance Team and **do not** complete a Data Protection Impact Assessment. Please email the completed screening to nelcsu.Information-Governance@nhs.net

Use of Personal Information			
Description of data: National and local data flows containing personal and identifiable personal information			
Personal Data	Please tick all that apply	Special Category Data	Please tick all that apply
Name	✓	Racial / ethnic origin	✓
Address (home or business)	✓	Political opinions	
Postcode	✓	Religious beliefs	✓
NHS No	✓	Trade union membership	
Email address		Physical or mental health	✓
Date of Birth	✓	Sexual life	✓
Payroll number		Criminal offences	
Driving Licence (shows date of birth and first part of surname)		Biometrics; DNA profile, fingerprints	
		Bank, financial or credit card details	
		Mother’s maiden name	
		National Insurance number	
		Tax, benefit or pension Records	
		Health, adoption, employment, school, Social Services, housing records	
		Child Protection	
		Safeguarding Adults	✓
Additional data types (if relevant)			

Lawfulness of the processing				
Conditions for processing for special categories: to be identified as whether they apply				
Condition		Please tick all that apply		
Explicit consent unless or allowed by other legal route	Explicit consent		Other legal route	✓
Processing is required by law				
Processing is required to protect the vital interests of the person				
Is any processing going to be by a not for profit organisation, e.g. a Charity				
Would any processing use data already in the public domain?				
Could the data being processed be required for the defence of a legal claim?				
Would the data be made available publically, subject to ensuring no-one can be identified from the data?				
Is the processing for a medical purpose?				✓
Would the data be made available publically, for public health reasons?				
Will any of the data being processed be made available for research purposes?				

The answers will not specifically identify the legality of the data flow; your responses to the questions below need to identify the specific legal route for processing.

Business Sensitive Data			
Financial	N/A	Procurement information	N/A
Local Contract conditions	N/A	(National contract conditions are in the Public domain)	
Decisions impacting:	One or more business function		N/A
	Across the Organisation		N/A
Description of other data collected			
N/A			

Answer all the questions below for the processing of Personal Confidential Data	
What is the justification for the inclusion of identifiable data rather than using de-identified/anonymised data?	The identifiable data is required in order to provide direct care to care home residents receiving emergency and/or urgent medical treatment in hospital.
Will the information be new information as opposed to using existing information in different ways?	The processing is about using existing information in different ways.
What is the legal basis for the processing of identifiable data? E.g. Conditions under the Data Protection Act 2018, GDPR, the Section 251 under the NHS Act 2006 etc. (See Appendix 1 for Lawfulness Conditions under the Data Protection Legislation).If consent, when and how will this be obtained and recorded? [1]	Article 6 1 E – Public Task Article 9 2 H – Provision of Health and Social Care Article 9 2 B '…social protection law…'

[1] See NHS Confidentiality Code of Practice Annex C for guidance on where consent should be gained. NHS Act 2006 S251 approval is authorised by the National Information Governance Board Ethics and Confidentiality Committee and a reference number should be provided

Where and how will this data be stored?	MCM is a SaaS (Software as a Service) solution and is hosted on the Microsoft Azure platform. The data is stored within the EU to ensure that GDPR and data protection security standards are not breached. Data on the servers is both backed up and replicated within the EU data centre network. To achieve this, PCS use the Microsoft Azure Geo Replication service. The Azure service is always fully up to date with the latest security patches and virus definition updates, ensuring further compliance with GDPR data protection legislation. Individuals' data is segregated by the organisation responsible for the individual / where they are receiving care, data is further segregated by the service to which they are living in or receiving care from. Any data held (including PDFs generated as part of the Red bag process – see below for how the PDFs are generated) are encrypted in transit and at rest. Data in transit is encrypted using standard HTTPS encryption over TLS. Data at rest is encrypted though 256bit AES encryption with encryption keys rotated regularly. The process for generating a digital red bag pdf by the paper-based care home is: 1.The care home administrator (with the care home manager) will open the MCM software and: a. Set-up the care home profile b. Upload a photo of each resident taken less than six months ago (note that the photo is stored on the care home administrator's PC which is password protected) c. Input key information (forename, surname, preferred name, DOB, gender, NHS number) d. Upload all the current red bag paperwork for every resident. (There is a paper-based file containing the completed paperwork for each resident) 2. When a resident is about to go to hospital, the lead carer will unlock the handheld device near the iBeacon, and then use it to take, and directly upload into the MCM software, a photo of the resident's: a. MAR chart sheet/s b. Carer's Escalation Record paperwork c. Any additional supplementary images (e.g. possessions list, pressure points/ulcers, skin damage) 3. Before the resident goes to hospital, the newly generated Red Bag hospital pack paperwork will be printed from the MCM software and put, together with

	the resident's key personal belongings and medication, into the Red Bag. 4. When the resident leaves for hospital, the Red Bag is given to the ambulance staff, and the lead carer returns to the iBeacon with the handheld device to send the hospital pack electronically to ESH by pressing the 'Save and Submit' button on the Hospital Pack screen 5. The lead carer checks that the hospital pack has been sent electronically by reviewing the handheld device and waiting for confirmation that the pack has been received by the ESH system. A care note is created as part of this process which will include the submission status. A manager or other user will be able to run a report for all hospital admission care notes and then can review where and when the data was sent and received by ESH. Please note that this process, and the MCM software, are included in the evaluation of the pilot. Further changes and developments to both are likely.
Who will be able to access identifiable data?	Relevantly qualified care home staff who are responsible for caring for the residents. PCS support staff at the request of users may require access to resident's data to provide the necessary support for making sure that the MCM software is correct. Access to residents' records by PCS staff is tracked as part of the record auditing process. Staff at ESH Trust when the paperwork is added to the hospital records.
Will the data be linked with any other data collections?	N/A
How will this linkage be achieved?	N/A
Is there a lawfulness conditions for these linkages?	N/A
How have you ensured that the right to data portability can be respected? i.e. Data relating to particular people can be	N/A

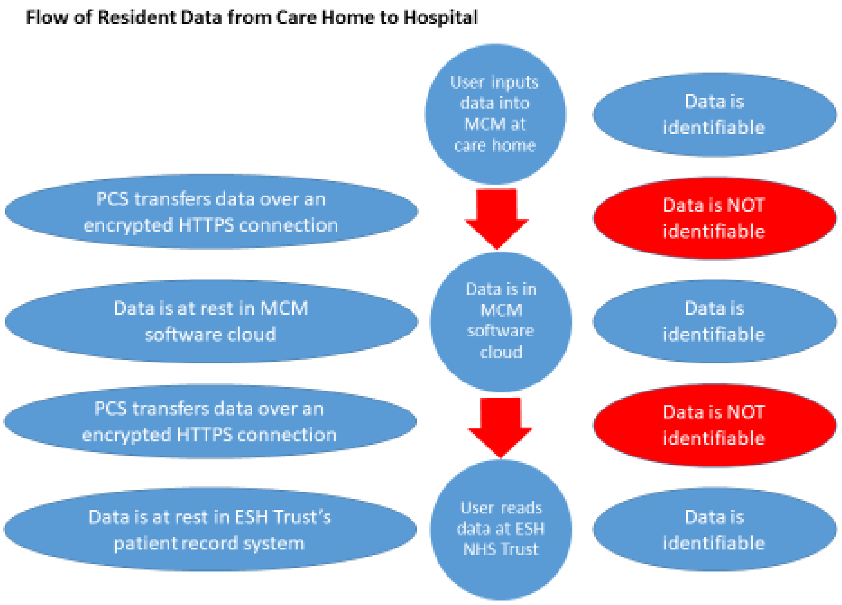
extracted for transfer to another Controller, at the request of the person to which it relates, subject to: • Receipt of written instructions from the person to which the data relates. • Including data used for any automated processing, And The transfer of the data has been made technically feasible. **N.B.** Transferable data does not include any data that is in the public domain at the time of the request. No data that may affect the rights of someone other than the person making the request can be included.	
What security measures will be used to transfer the data?	Data is transferred over an encrypted HTTPS connection
What confidentiality and security measures will be used to store the data?	For users of the MCM software, data at rest is encrypted though 256bit AES encryption with encryption keys rotated regularly. In addition, access to the pdf files is authenticated through a 704bit access key. The ESH Trust uses a secure patient record system. The Trust's patient record system is called iSOFT Patient Manager or iPM and its electronic health record/EPR is iSOFT Clinical Manager or iCM.
How long will the data be retained in identifiable form? And how will it be de-identified? Or destroyed?	Care providers are required to keep records of residents care plans and evidence of care provided. For users of the MCM software, residents' records can be archived in MCM once they no longer receive care from a provider to restrict further processing. Adult services will be retained in MCM for 8 years, in line with the recommended guidelines set out by the Information

	Governance Alliance: Records Management Code of Practice for Health and Social Care 2016. Data held is categorised by person and the type of data. The ESH Trust follows the same Information Governance Alliance guidelines.
What governance measures are in place to oversee the confidentiality, security and appropriate use of the data and manage disclosures of data extracts to third parties to ensure identifiable data is not disclosed or is only disclosed with consent or another legal basis?	Data will only be used for the stated purpose and accessed by authenticated users. It can only be transferred to ESH Trust when a resident goes to hospital from the care home. The transfer of data is initiated only by a member of staff at the care home. All Stakeholders have the necessary policies and procedures in place to provide this function effectively, where relevant.
If holding personal i.e. identifiable data, are procedures in place to provide access to records under the subject access provisions of Data Protection Laws? Is there functionality to respect objections/ withdrawals of consent?	This is the responsibility of each care home as it is the data controller which responds to data access requests. All data held about an individual will be available and controlled by system users. The care homes have the relevant policies and procedures in place to ensure that the subject access process is adhered to.
Are there any plans to allow the information to be used elsewhere either in NEL, wider NHS or by a third party?	No
Will the fair processing notices in relation to this data be updated and ensure it includes: • ID of controller • Lawfulness conditions of processing • Categories of personal data • Recipients, sources or categories of recipients of the data: any	All stakeholders involved in this project have the relevant Privacy Notices in place which are available to the data subjects. All ICO registrations are up to date. ESH Trust ICO Registration number: Z6690929 Registration expires: 29 April 2019 PCS ICO Registration number: ZA311564 Registration expires: 28 January 2020 Belmont House privacy notice:

sharing or transfers of the data (including to other countries) - Any automated decision making - Retention period for the personal data - Existence of data subject rights, including withdrawal of consent and data portability	Privacy Policy Caring Homes Group.pdf ICO Registration number: Z2815302 Registration expires: 20 July 2019 Southcare Homes (Grasmere) privacy notices: ICO Registration number: Z3455187 Registration expires: 29 November 2019 SC - Privacy Notice (Friends Relatives) Ja SC - Privacy Notice (Service Users) Jan 20 SC - Privacy Notice (Staff) Dec 2018.docx
The data must be able to be easily separated from other datasets to enable data portability (see previous questions), audit of data relating to specific organisations and to facilitate any requirements for service transitions.	PCS: Data is segregated by organisation and person refrerence to allow for data portability. PCS would be able to assist with this on a case by case request. ESH Trust: This data is separated as it is held as a separate "Information Type" in our Document Management system. We can audit who has retrieved this data from within our organisation if this is needed.

Are there any new or additional reporting requirements for this project?	**Yes/No**
	Yes*
*This is only for the testing of the 'proof of concept' for evaluation purposes	
- What roles will be able to run reports?	
Technical Support roles in PCS and ESH	
- What roles will receive the report or where will it be published?	
The project manager for this work and hospital staff	

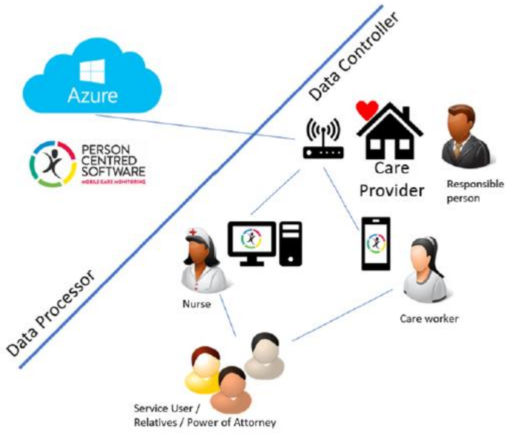
• Will the reports be in person-identifiable, pseudonymised or anonymised format?
The patient (care home resident) will be anonymous, whilst the hospital staff will be identified
• Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format?
Redacted
• If this new/revised function should stop, what are the plans for how the information will be retained / archived/ transferred or disposed of? or additional reporting requirements for this project?
If the digital red bag paperwork is stopped or is not sent, then: • The hard copy will be used by the ESH staff and either will be contained in the patient's notes or returned to the care home with the resident, as happens now. The storage will follow the ESH Trust's procedure • For the paper-based care home, procedures will be put in place to terminate its contract, and remove equipment, access to the software, and all data. • For the care home that uses MCM software the paper-based version of the red bag pack will continue to be sent to the hospital inside a person's red bag. The contract with PCS will continue.

Are multiple organisations involved in processing the data? If yes, list below		**Yes/No**
		Yes
Name	Controller and/or Processor?	Completed and compliant with the IG Toolkit or with the DSP Toolkit[2]
		Yes/No
Belmont House	Controller	Yes, the IG Toolkit by Caring Homes Group
Grasmere Rest Home	Controller	No – Work in progress**
Person Centred Software Ltd	Processor	Yes, the DSP Toolkit full assessment completed
Epsom and St Helier University Hospitals NHS Trust	Controller	Yes, the DSP Tookit, baseline (standards met) completed
Has a data flow mapping exercise been undertaken? If yes, please provide a copy, if no, please undertake – see Note 4 for guidance		Yes/No
		Yes, see below
 Flow of Resident Data from Care Home to Hospital User inputs data into MCM at care home Data is identifiable PCS transfers data over an encrypted HTTPS connection Data is NOT identifiable Data is at rest in MCM software cloud Data is in MCM software cloud Data is identifiable PCS transfers data over an encrypted HTTPS connection Data is NOT identifiable Data is at rest in ESH Trust's patient record system User reads data at ESH NHS Trust Data is identifiable		

[2] The Data Security and Protection Toolkit is a self-assessment tool provided by NHS Digital to assess compliance to the Information Governance

Is Mandatory Staff Training in place for the following?	Yes/No	Dates
• Data Collection:	Yes	On Appointment
• Use of the System or Service:	Yes	On Appointment
• Collecting Consent:	N/A	
• Information Governance:	Yes	Annually

** Grasmere Rest Home is being supported to comply with the DSP Toolkit by South West London Health and Care Partnership which is working closely with the home and its group manager. At 23 January 2019, there are four items to complete to achieve Standards Met which includes one for Entry Level. The Group Manager is working to achieve these.

Describe the Information Flows The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows.	
Does any data flow in identifiable form? If so, from where, and to where?	Identifiable data is entered into MCM software by the user. Data is transferred to hospital system using https encryption and therefore is not identifiable. Data is identifiable in the hospital system. See flow chart above.
Media used for data flow? (e.g. email, fax, post, courier, other – please specify all that will be used)	When a resident is created in MCM, the file information is usually provided by the resident or the representatives during the admission process and entered by staff at the care home / service. On-going care planning and evidence of care is entered by the staff supporting the individual.  Data Controller Azure PERSON CENTRED SOFTWARE MOBILE CARE MONITORING Care Provider Responsible person Nurse Care worker Service User / Relatives / Power of Attorney Data Processor Data flow between the care home and the hosptial is transferred using secure web services using the HL7 message sets.

Data Protection Risks

List any identified risks to Data Protection and personal information of which the project is currently aware. Risks should also be included on the project risk register.

Risk Description (to individuals, to the NEL or to wider compliance)	Current Impact	Current Likelihood	Risk Score (I x L)	Proposed Risk solution (Mitigation)	Is the risk reduced, transferred, or accepted? Please specify.	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Sending the incorrect digital red bag record to ESH Trust	3	3	12	Ensure MCM software and Care Homes have a double checking process in place.	REDUCED	
Cyber Attack	2	2	4	The MCM platform is penetration tested to protect against service and data attacks by a "check registered" 3rd party on a bi-annual basis; including certification of the testing conducted.	REDUCED	
Member of ESH Trust staff access the patient information inappropriately	2	2	4	Part of the staff contract is code of confidentiality Regular audits	REDUCED	

Loss of password / sharing password	4	2	8	Individual passwords are used in Belmont House currently and therefore this is less of a risk there. In Grasmere, to access the online MCM software, there will be user names and passwords, which the care home manager and administrator are used to having. The iBeacon is designed to replicate paper security (which is essentially access to the paper files in a physical location). With the iBeacon, access to the application can only be made using an authenticated app at the same time as being within close proximity to the iBeacon (which will be placed in an area in the home where access is controlled). Therefore the use of iBeacon removes the need for passwords.	REDUCED	

Approval by IG Team/Information Security

Risk Description	Approved solution	Approved by	Date of approval

Actions to be Taken		
Action to be taken	Date of Completion	Action Owner
DPIA completed by SW London HCP	03/12/2018	Lucy McCulloch
DPIA reviewed with comments, by IG SME	10/12/2018	Claire Clements
DPIA re-reviewed by SWL HCP and returned to IG SME	17/12/2018	Lucy McCulloch
DPIA re-reviewed by IG SME – comments added and returned to SWL HCP	02/01/2019	Claire Clements
DPIA returned to the IG SME for review	09/01/2019	Lucy McCulloch
DPIA re-reviewed by IG SME – further comments added and returned to SWL HCP	11/01/2019	Claire Clements
DPIA reviewed by ESH IG lead – further comments added and returned to SWL HCP	11/01/2019	Paul Kenny
DPIA re-reviewed by SWL HCP and returned to IG SME and ESH	15/01/2019	Lucy McCulloch
Following a meeting with IG SME, the DPIA re-reviewed	17/01/2019	Lucy McCulloch
Following a phonecall and email correspondence with Paul Kenny, revised the sign-off names	24/01/2019	Lucy McCulloch
Inserted new privacy notices for Southcare Homes for service users and relatives/friends and updated their ICO number. Added in text re status of this pilot.	24/01/2019	Lucy McCulloch

Consultation requirements

Part of any project is consultation with stakeholders and other parties. In addition to those indicated "Key information, above", please list other groups or individuals with whom consultation should take place in relation to the use of person identifiable information.

It is the project's responsibility to ensure consultations take place, but IG will advise and guide on any outcomes from such consultations.

Other people and organisations consulted are:

- Andrew Coles and Simon Papworth at Person Centred Software
- Joyce Rochester and Daren Veal, Epsom and St Helier Hospitals University Trust
- Tony Afuwape and Renata Leppich, SWL HCP digital team members
- Sutton CCG
- London Borough of Sutton

Further information/Attachments
Please provide any further information that will help in determining Data Protection impact.
See note 5 for examples

All information is embedded in the document or is linked to the internet

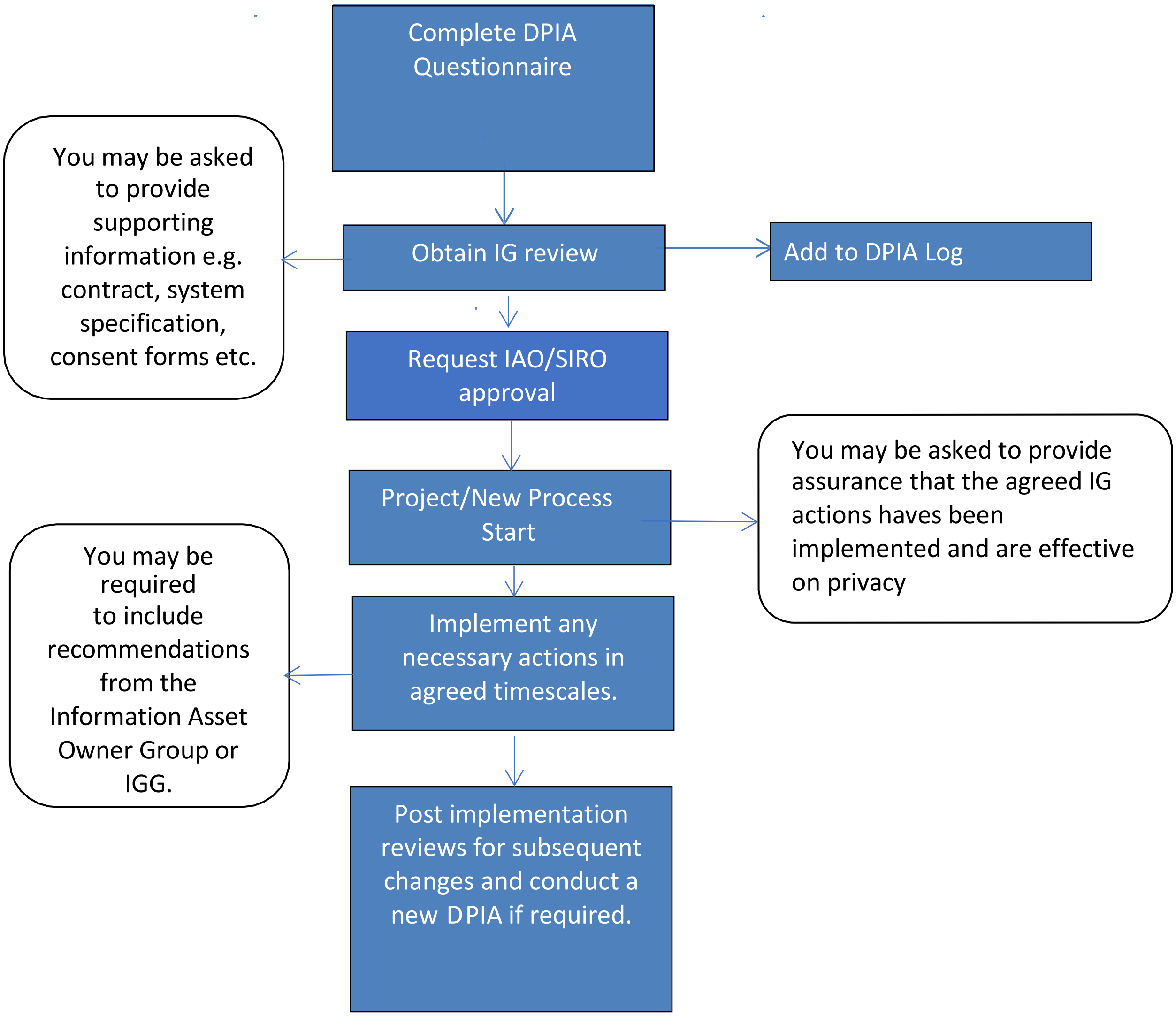
IG Team comments:

Following review of this DPIA by the Information Governance Team, a determination will be made regarding the Data Protection impact and how the impact will be handled. This will fall into three categories:

1. No action is required by IG excepting the logging of the Screening Questions for recording purposes.
2. The questionnaire shows use of personal information but in ways that do not need direct IG involvement – IG may ask to be kept updated at key project milestones.
3. The questionnaire shows significant use of personal information requiring IG involvement via a report and/or involvement in the project to ensure compliance.

It is the intention that IG will advise and guide those projects that require IG compliance but at all times will endeavour to ensure that the project moves forward and that IG is not a barrier unless significant risks come to light which cannot be addressed as part of the project development and will need to be escalated to the NEL CSU Senior Information Risk Owner- SIRO, David Thomas, for approval.

The DPIA Process



Complete DPIA Questionnaire

Obtain IG review

Add to DPIA Log

You may be asked to provide supporting information e.g. contract, system specification, consent forms etc.

Request IAO/SIRO approval

Project/New Process Start

You may be asked to provide assurance that the agreed IG actions haves been implemented and are effective on privacy

Implement any necessary actions in agreed timescales.

You may be required to include recommendations from the Information Asset Owner Group or IGG.

Post implementation reviews for subsequent changes and conduct a new DPIA if required.

Please email entire completed document to nelcsu.Information-Governance@nhs.net

Sign off by Person Centred Software Limited

IG review

IG Staff Name and Job Title: Andrew Coles, Product Management
Signature: Approval via email, Tue 29/01/2019 10:09

Date: 29/01/2019

Information Asset Owner (IAO) approval (for low to medium risk processing)

IAO name: N/A

Signature:

Date:

SIRO approval (for high risk processing)

SIRO Name and Job Title: Simon Papworth, Chief Executive
Signature: Approval via email, Tue 29/01/2019 15:27

Date: 29/01/2019

Sign off by Epsom and St Helier Hospitals NHS Trust

IG review
IG staff name: Paul Kenny, Information Governance Manager & DPO
Signature: Approval via email, Wed 30/01/2019 14:28

Date: 30/01/2019

Caldicott Guardian
CG name: Dr Vipula De Silva, Consultant Nephrologist
Signature: Approval via email, Wed 30/01/2019 16:54

Date: 30/01/2019

Information Asset Owner (IAO) approval (for low to medium risk processing)
IAO name: Hilary Bennett, Head of Capacity Management
Signature: Approval via email, Fri 01/02/2019 16:09
Date: 01/02/2019

SIRO approval (for high risk processing)
SIRO name: Peter Davies, Director of Corporate Services
Signature: Approval via email, Wed 30/01/2019 15:33

Date: 30/01/2019

Sign off by others

IG review
IG Staff Name and Job Title: Claire Clements, Information Governance SME Manager, NEL CSU
Signature: approval via email, Tue 29/01/2019 10:36

Date: 29/01/2019

IG review for Belmont House Care Home, Caring Homes Group
SIRO Name and Job Title: Sundeep Sagoo, DPO for Caring Homes Group
Signature: approval via email, Wed 30/01/2019 10:38

Date: 30/01/2019

Information Asset Owner (IAO) approval for Belmont House Care Home
IAO Name and Job Title: Arthur Tanare, Care Home Manager
Signature: approval via email, Thu 31/01/2019 09:41

Date: 31/01/2019

SIRO approval for Belmont House Care Home, Caring Homes Group
SIRO Name and Job Title: Peter Hill, Group Chief Financial Officer
Signature: Due on Monday 4 February 2019

Date:

Information Asset Owner (IAO) approval for Grasmere Rest Home
IAO Name and Job Title: Moyra Hillman, Care Home Manager
Signature: approval on hold due to illness

Date:

SIRO approval for Grasmere Rest Home
SIRO Name and Job Title: Tracey Austin, Group Manager
Signature: approval via email, 29 January 2019 18:56

Date: 29/01/2019

Approval from Sutton CCG IG Steering Group
Signature: approval via emails from three out of four members, the fourth being on leave, Tue 29/01/2019 16:34

Date: 29/01/2019

Appendix 1- The conditions (the legal basis) for processing Personal Data under the Data Protection Legislation

The conditions for processing Personal Data and Sensitive Personal Data the Data Protection Legislation, Data Protection Act 2018 and General Data Protection Regulation (EU) 2016/679 as referenced in this Act – identified in this documentation as the Data Protection Legislation.

Definition of Personal Data and Special Category Data

Data:

- The Data Protection Act defines data as:
  - Information which is being processed automatically in response to instruction
  - Information recorded as part of a highly structured filing system (e.g. an individual with limited knowledge of the filing structure could logically retrieve relevant information)
  - Recorded information held by a public authority
  - Information that forms part of an accessible record (health, educational, public record)

Personal Data:

- Personal data means data which relates to a living person who can be identified from that set of data or who could be identified if that data was combined with other information either available or likely to become available.
- This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Special Category Data

The GDPR refers to sensitive personal data as “special categories of personal data” (see Article 9). The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

Special Categories of personal data includes Information relating to the data subjects’:

- racial or ethnic origin,
- political opinions,
- religious beliefs or other beliefs of a similar nature,
- trade union membership,
- physical or mental health or condition,
- sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

The Data Protection Act (DPA) outlines 6 principles for handling Personal Confidential Data (PCD), with 2 additional safeguards:

1. Data must be processed fairly and lawfully
2. Data must be obtained and processed only for one or more specified and lawful purposes
3. Date must be adequate, relevant and not excessive in relation to the purpose
4. Data must be accurate and kept up to date
5. Data must not be kept for longer than is necessary
6. Appropriate technical and organisational security measures for the data must be in place

Safeguards:

1. Data must be processed in accordance with the rights of data subjects
2. Sensitive Data must only be processed with legal compliance to the Act, referenced to a current policy. e.g. Can only be processed in a country or territory outside the United Kingdom unless adequate levels of protection are in place, within statutory functions.

Supporting Guidance for Completion of the Data Protection Impact Assessment	
1.	Information Asset E.g. Operating systems, infrastructure, business applications, off-the-shelf products, services, user-developed applications, devices/equipment, records and information (extensive list).
2.	Person Confidential Data
	Key identifiable information includes: • patient's name, address, full post code, date of birth; • pictures, photographs, videos, audio-tapes or other images of patients; • NHS number and local patient identifiable codes; • Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.
3.	New use of information could include: - consistent with DPIA Introduction

	Setting up of a new service. The Commissioning of a new service Data Extracts Setting up a database or independent Patient System Reports
	Examples of changes to use of information could include:
	Moving paper files to electronic systems Collecting more data than before Using Data Extracts for a different purpose Additional organisations involved in information process Revisions to systems, databases (including merges) or spread sheet reports
4.	Data Flow Mapping
	A Data Flow Map is a graphical representation of the data flow. This should include: • Incoming and outgoing data • Organisations and/or people sending/receiving information • Storage for the 'Data at Rest' i.e. system, filing cabinet • Methods of transfer
5.	Examples of additional documentation which may be required (copies):
	• Contracts • Confidentiality Agreements • Project Specification • System Specifications (including Access Controls) • Local Access Controls Applications • Information provided to patients • Consent forms