Introduction

A Data Protection Impact Assessment (DPIA) is a legal requirement for certain kinds of projects and activities. These include:

- ✓ new and innovative technologies such as artificial intelligence;
- ✓ where the data being used is sensitive and relates to an individual's health
- ✓ any systematic and extensive profiling
- ✓ monitoring of public areas
- ✓ where decisions are made to deny or allow access to services
- ✓ matching and combing data from more than one source
- ✓ where the data subject is considered vulnerable i.e. children, mental health
- ✓ automated decision making with significant effect upon individuals

The aim of a DPIA is to identify and assess the risk of an activity or project and the impact it may have upon an individual. It helps the Trust act in a lawful and risk-minimising way. DPIA's once complete and approved are retained by the Trust as a record of a system/process.

You should involve your Divisional Information Assets Assistant in the completion of your DPIA and it must be signed by them as evidence they are aware of all processing, data flows, information assets and associated risks.

A DPIA is a dynamic process that should be revisited as systems/processes develop and when nature, scope or purpose of the processing of data changes.

Who should complete a DPIA?

The Trust is responsible and remains ultimately accountable for ensuring that the DPIA is carried out.

A Divisional NUH Project/Senior Manager/Sponsor supported by **Divisional Information Assets Owners (IAO) and Information Assets Assistants (IAA**) should own and complete this DPIA, and then submit the DPIA to the Information Governance Team for review IGNotifications@nuh.nhs.uk. IAA's are required to initially sign the document before submission to evidence their involvement.

Relevant stakeholders (internal and external) should be consulted throughout the DPIA process to assist in identifying privacy risk.

What if I need help?
The Information Governance Team are able to provide advice and assistance to NUH Project/Senior Manager/Sponsor's and Divisional Information Assets Assistants if required.

IMPORTANT – INSTRUCTION ON COMPLETING ASSESSMENT

PLEASE COMPLETE EACH QUESTION FULLY. IF YOU THINK A QUESTION DOES NOT APPLY TO YOUR PROJECT/ ACTIVITY, INSERT N/A AND EXPLAIN WHY. DO NOT LEAVE UNANSWERED QUESTIONS.

Project/System/Process Name *[Use a unique name and refer to in all correspondence]*	Nottingham Pre-Hospital Frailty Network Casefile Review

DPIA reference number *[Issued by Information Governance Team]*	

Key Personnel

	NUH Business/ Operational lead	ICT lead (if applicable)	Supplier lead (if applicable)	Information Asset Owner/Assistant (see List of Information Asset Owners and Administrators) (MUST SIGN STEP 9)	*You will need to complete all contact details in this section.*
Name	Steve Rutter	n/a	n/a	Jane Swift	
Role	Consultant			Information Manager	
Email					
Phone					

Step 1: Aim of project/activity being undertaken

1. What is it that is being planned?

Provide a brief description and/or embed an Additional Service Request, Project Initiation Document or proposal.	We intend to complete a 50 case note review, where 30 patients conveyed by EMAS to NUH, and 20 patients conveyed to SFHFT, that meet a set criteria are identified and their journey through the system is reviewed to identify any areas of learning and key themes. The NHS numbers for the identified patients will need to be sent via nhs.net to EMAS to allow EMAS to find the same patients in their own system, but no other information about the patient will be shared between EMAS, NUH, or SFHFT. EMAS will then complete a pseudo-anonymised spreadsheet including information on the patient's journey and return it to Alice Clayton from the Pre-Hospital Frailty Network. Both NUH and SFHFT will then have a Teams call with the Pre-Hospital Frailty Network, the CCG, and colleagues from the community, where patients 1-50 will be discussed but no NHS number or any other identifiable information will be discussed. Only the acute trust will have any identifiable information about their patients. The key themes and learning from the case note review will then be analysed by the Pre-Hospital Frailty Network.

2. What is the nature of your relationship with the data subject whose data will be used?

For example, do you provide direct care to the data subjects, are they your patients?	All patients will be retrospectively selected from Nov-21. Some of the staff on the call from the acute hospital may have been involved in the patients care, but this project will have no impact on the direct care of any of the patients discussed. Providers other than the acute trust and EMAS will not know who the patients are.

3. Why are we doing it?

Summarise why there is a need for implementation or change and the benefits it will realise.	We are hoping to gain insights into which patients in the future could have benefitted from being cared for in a Virtual ward/Home First+ service and understand what the characteristics/themes or enhanced level of input may be required to succeed in a future virtual ward implementation.

4. Individuals need to be told how their information is processed.

Is this covered by an existing fair processing information or leaflet? If Yes, provide details. If No, go to Q5	Sherwood Forest Hospitals (sfh-tr.nhs.uk) Yes, our privacy notice says: How the NHS and care services use your information We are one of the many organisations working in the health and care system to improve care for patients and the public. Whenever you use a health or care service, such as attending Accident & Emergency or using Community Care services, important information about you is collected to help ensure you get the best possible care and treatment. The information collected about you when you use these services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with: • improving the quality and standards of care provided • research into the development of new treatments • preventing illness and diseases • monitoring safety • planning services. This may only take place when there is a clear legal basis to use this information. All these uses help to provide better health and care for	*Check the Trusts Fair Processing Notice by viewing the external SFH Internet.*

	you, your family and future generations. Confidential patient information about your health and care is only used like this where allowed by law. Most of the time, anonymised data is used for research and planning so that you cannot be identified in which case your confidential patient information isn't needed. You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do choose to opt-out your confidential patient information will still be used to support your individual care.	

5. Have they been informed and consented to this use?

N.B. this is consent to the processing of their personal data, not consent to treatment

a. Have you consulted the data subject or their representative about using this data? If not, please explain why you haven't consulted them?	No, as the project doesn't allow for the time to reach out to patients individually. However SFHFT will check National Data opt-outs to ensure we do not use patients who have opted out.
b. Please provide details and an example of how this consent to processing of their data was given? (Preferably embed document)	N/A

c. Explain why you believe they would consider the proposed new use of their data as being reasonable or expected?	This project has the potential to improve care for all patients in a similar position to them in the future. No new information about their care would be shared across providers. Only the acute trust and EMAS would have their identifiable information, and no other information would be shared between these organisations.
d. How will you tell patients/staff how their data is being used and if not, why not?	Patients are told about the use of their personal data via the privacy notice.

6. Has an assessment been made that the information collected is the minimum required to meet the aim of the project?

a. Use of data should not be the first resort if the objective can be achieved without its use. You must justify why the use of all the data is necessary and proportionate. For example, do you need to use all the fields, can you not achieve the same objective with fewer data fields and/or a smaller data set?	The only identifiable information shared will be NHS number, and this is the bare minimum we can share to be able to know all parties are referring to the same patient.
b. Has consideration been given to how the same objective or outcome may be achieved without using this data or using less data or employing a different method - explain in full?	There is no way to gain insight into the current patient journey across EMAS and the acute trust without sharing the NHS number for the set number of patients, to ensure we are able to follow a singular patients complete journey.

7. Is this processing using novel technology or for a novel purpose that would be of public interest or attract criticism. Explain your reasons?

a. Is the technology or activity new to the Trust or is it a recent development?	No, casefile reviews are a common activity.
b. Where else is the technology used, have they completed a DPIA that may	No novel technology is used.

be useful for background information, if so please provide (embed document)?	

Step 2: Data description and use

8. What type of data is being processed?

Fully describe ALL the data that will be used and justify why they are needed. Detail what data fields are being used e.g. NHS No, date of birth, name etc.?	**Data item**	**Why is it required?**
	NHS number	**To be able to identify the patient in different organisations, to track their journey through the services**
	Age	**To gain insight into the age of the patients that may have been suitable for a virtual ward.**

9. Does this include any of the following special categories of personal data?

Data concerning health	☒

Data concerning sex life or sexual orientation	☐
Genetic or biometric data	☐
Racial or ethnic origin	☐
Religious or philosophical beliefs	☐

10. Approximately how many individuals will be in the dataset?

<100	☒	100-500	☐	500-1,000	☐	1,000-10,000	☐	10,000-50,000	☐	>50,000	☐

11. What volume of data will be involved?

How large and expansive are the records sets being used, what will it consist of? What geographical area will the data be drawn from or cover?	The patient's clinical notes will be accessed by the clinician at the acute site. We will talk through the notes and identify timings/opportunities for alternative care.

12. What is the source of this data?

a. If the data is being taken from an existing system, identify what system that is and what was the originally purpose that data was collected for? How will this data be accessed?	The data will be accessed by the clinician logging into the patient notes system.
b. If it new data that is being collected, describe how this data collection will be done i.e. electronic form, paper form etc.?	Alice Clayton will collect pseudo-anonymised data in an Excel file. The clinician will hold the NHS number, and each will be associated with a pseudoID generated by the internal analytical team.

13. How will this data be used?

a. Will this data be used or combined with other data sets, if so what are these other data sets?	The pseudo-anonymised data will be combined with data from EMAS, but no identifiable information will be available to those who can access the combined data.
b. What will this data show you that is relevant to the project aim and purpose?	This will allow us to see the patient's whole journey, from ambulance to discharge from the acute.

14. Duration of processing

What is the duration of this processing? Is this one-off processing or will it continue for a specified period?	This is a one-off processing.

15. How long will the data be kept and how will it be deleted?

a. NHS data needs to be retained in accordance with the NHS Records Management Code of Practice. Has provision been made to ensure you are able to accommodate this? If No, describe how the data will be stored.	Only pseudo-anonymised data will be kept, and this will be deleted upon completion of the analysis – this will likely be 2 weeks.	You will need to evidence that intent is to retain data only for as long as necessary and within the NHS Records Management Code of practice. You can look up the necessary retention period in the schedule here
b. If data is being processed by a third party, how will we ensure data is deleted when required?	Alice Clayton from the Pre-Hospital Frailty Network will confirm once she has deleted the data.	Appropriate evidence would be an embedded copy of the contract or agreement containing this detail

16. How has the required data been minimised?

You are required to minimise the amount and level detail of any data set. For example, dates of birth should not be used where age would provide sufficient information to achieve the project aim.	Yes, we will be using age rather than DOB. NHS number is the only identifiable information shared, and this will not be stored by anyone outside of EMAS, NUH or SFHFT.

17. Is the data is anonymised or pseudonymised in any way, please explain why and how this has been done?

Where possible, data should be anonymised or pseudonymised as far as possible. Has this been considered or done and if so how? What steps have been taken to minimise the risk of re-identification of anonymised or pseudonymised data?	Yes, we will be using age rather than DOB. NHS number is the only identifiable information shared, and this will not be stored by anyone outside of EMAS, NUH or SFHFT.

Step 3: Data Security

All personal data must be stored, transmitted and deleted securely.

NOTE: The supplier or third party may be able to advise on this section. Please provide details for all questions.

18. Where will these data be stored?

a. Will the data be stored on SFH servers or servers external to the Trust?	The NHS number will need to be stored temporarily by EMAS. The list will be sent from SFH to EMAS via secure email (nhs.net).
b. If external, where will it be stored, will this be the UK, EU or elsewhere?	This will be in the UK
c. Will the storage be controlled by another party such as a product/ platform supplier?	No
d. If the data storage or processing is being done by a third party, what certifications do they hold i.e. ISO 27001 or other certifying bodies? When were they, and the proposed storage mechanism, subjected to an external penetration test and is a report available? (Please embed any documentary evidence)	EMAS do not have ISO27001 or CE+ which are data security standards. However EMAS are registered with the ICO (data protection regulators) and complete the data security and protection toolkit annually (approaching standards).

e. If the data is stored on a cloud platform, please provide details, and complete and embed/attach a cloud security questionnaire.	n/a

	Can the supplier demonstrate compliance with any of the following standards? If YES please provide further information e.g. date achieved and a copy of the certificates		
		Yes	No
	Cyber Essentials Plus		No
	ISO 15489 Records Management		No
	ISO 27001 Information Security Standards		No
	ISO 9001 Quality Management Systems		No

19. How will this data be secured during storage and when being moved?

a. Will it be encrypted when stored and/or moved, if so what type of encryption will be employed?	The list of NHS numbers will be emailed to EMAS using secure email (nhs.net).
b. Will it be on a server protected by firewall and network intrusion detection?	Yes

c. What technical controls are in place to prevent hacking of the data by unauthorised persons?	NHSmail/N365 conforms to the DCB1596: Secure email information standard
d. When being moved will it be secured through encrypted file transfer, secure transmission through SLL/TLS/SHS, please explain the specific technical standards that will apply?	TLS ensures the security of the information being processed via NHSmail.  o365-secure-email-configuration-v1.3_final

20. Who will have access to this data and how will this access be controlled?

a. Will the data be kept on a system that is password controlled, what is the password length and how often does it have to be changed? Who will administer these access controls?	It will be on NHSmail and any passwords will meet their requirements.
b. What other security measures are in place, such as physical security, multiple factor authentication?	Any physical notes collected will be kept behind a swipe card access door on site. All electronic notes and information will be held in secure folders on the shared drive where folders and access to individuals is regularly reviewed.

21. If you are using devices such as laptops to access data, how are these secured and managed?

Are all laptops and PCs encrypted and protected and how this is done?	n/a they should be using trust computer

22. What will happen to the data at the end of the project/activity or end of contract with a third party? Will it be returned or deleted and how will this be done?

Most contracts specify what happens to data at the end of contract. If this is not subject to contract, how will you ensure the data held by any third party is deleted? Embed extract of contract as	Once EMAS have identified the patient notes associated with the NHS number sent to them, they will delete the email containing the NHS numbers. All other data is pseudo-anonymised but will be deleted once the analysis is completed.

necessary with highlighted sections.	

23. Is this data an attractive target for criminals and hackers; does it contain information that may be used for identity/financial fraud or reveal a person possibly being vulnerable to exploitation?
Rate its attractiveness from 0 to 10 below.
If this is a risk describe how you will manage it in Step 8.

For Guidance visit:
https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

Not at all attractive 0 Highly attractive 10	Score (please highlight) : 0 1 2 3 4 5 6 7 8 9 10

Step 4: Data Use and Sharing

24. Will this data be shared with anyone else?

a. If yes, explain who these other parties are and why the data is being shared?	The pre-hospital frailty network are facilitating the casefile review and will be doing the analysis, but will not have access to any identifiable information (e.g. NHS number)
b. What is the statutory reason for this sharing?	They are analysing the information as they have skills supporting this activity.

25. Are other people processing this data?

a. If a third party such as a company is storing or otherwise managing or using our data, please explain what they doing and why they are doing it?	EMAS will be receiving the NHS numbers. They will then use this number to identify the patient in their own system.
b. If we are using a third party product that requires maintenance where they access our networks, explain how this	n/a they will not access your networks

will be managed (will they remotely connect, how will this access be managed).	

26. Describe the data flow?

a. Please embed or attach a simple flow map or visual description of how the data is collected, moved and used?	The patient NHS numbers will be identified by an analyst at NUH, then emailed to an EMAS colleague who will be able to identify that NHS number in their own data.
b. Are there security or data protection concerns in any of the data flow stages you identify? If so, please indicate where and what steps you taking to reduce these risk?	The email could be sent to the wrong person, but the sender should send a tester email first.

Step 5: Processing by or with a third party

a. If you are using a third party company or organisation to process, store or otherwise interact with this data, what is the arrangement between the Trust and the third party concerned?	The pre-hospital frailty network have been commissioned by NHSE to support Nottingham in reducing conveyance of frail older people to hospital.
b. What activities will the third party carry out i.e. storage, transport, processing of data on their platform?	They will collect pseudo-anonymised data via a Teams call with the acute site, with a clinician looking through the patient notes. They will then analyse this information for key themes and present the findings back to the site.
c. If this is carried out under a contractual agreement, please provide a copy of the contract and any other documents covering this arrangement. (Please embed docs into assessment)	n/a

d. What steps or measures will you put in place to manage these risks? What measures will you take to ensure processors comply? PLEASE ATTACH COPIES/ RELEVANT SECTIONS OF ANY CONTRACT/ AGREEMENT.	They have completed the DPIA, and we are working with their IG team.
e. If the data is being processed outside of the UK, please explain where?	no
f. If the data is processed outside of the EEA, what safeguards will be in place?	no

Step 6: Consultation

Consider how to consult with those who have an interest in this project/system:

a. Describe when and how you will seek individuals' views or justify why it's not appropriate to do so.	The pre-hospital frailty network (PHFN) will be providing insight alongside the analysis.
b. Who else do you need to involve within your organisation?	NUH Geriatrian who can access the patient notes, NUH analyst who can identify the patients suitable.
c. Do you need to ask your data processors to assist?	Alice Clayton from the PHFN will be liaising with an NUH analyst.
d. Do you plan to consult information security experts, or any other experts?	No

Step 7: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

a. What is your lawful basis for processing? You should select the single most appropriate basis.	Yes	No

b. *(In the unlikely event that you are not processing any personal data then a. is not relevant)*		
The data subject has given consent to the processing of his or her personal data for one or more specific purposes	☐	☒
Processing is necessary for the performance of a contract	☐	☒
Processing is necessary for compliance with a legal obligation to which the controller is subject;	☐	☒
Processing is necessary in order to protect the vital interests of the data subject	☐	☒
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested the controller	☒	☐
Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party NB. Not for public bodies.	☒	☒
If you are processing special category data e.g. health (see Step 2 Question 9) then you will need to satisfy a GDPR Article 9 condition. You should select the single most appropriate basis.	Yes	No
Processing is necessary for the purposes of preventative or occupational medicine…, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems	☒	☐
Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health	☐	☒
Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes	☐	☒
The data subject has given explicit consent to the processing of those personal data for one or more specific purposes	☐	☒

c. Explain how the processing actually achieves your purpose?	It allows us to identify opportunities for alternative care options e.g. a virtual ward. Once we have identified these opportunities, we can plan for future improvements.
d. Is there another way to achieve the same outcome, give details of alternative you have rejected?	No

e. How will you prevent function creep, what are the governance arrangements around this activity/project?	A clear plan has already been agreed.
f. How will you ensure high standards of data quality, please explain why all the data fields are necessary to achieve the objective?	We need to share the NHS number from SFH to EMAS to ensure the same patient is being discussed. All other data fields are necessary to help us understand future opportunities for virtual wards, and the types of patients that would be suitable.
g. Please explain why a smaller amount of data cannot be used?	30 patients from SFH is sufficient to provide themes that could be generalisable across the population. Some patients may also need to be excluded if the notes cannot be located on the day etc.
h. What information will you give individuals informing them of what you are doing with their data? How will you help to support their rights? PLEASE EXPLAIN YOUR THINKING.	Patients will not be informed that we are using their information. Only NHS number will be shared, no personal information that can be attributed back to them.
i. Does the National Data Opt-Out apply (allows patients to opt out of their confidential patient information being used for research and planning)? Guidance for health and care staff - NHS Digital	Yes this does apply. SFHFT will follow their procedure https://www.sfh-tr.nhs.uk/media/11057/ig-011-national-data-opt-out-for-clinical-audits-and-research-procedure.pdf

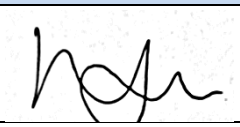
Step 8: Identify, assess and mitigate risks

Risk ref.	Risk	Consequence(s)	Risk rating now			Mitigation/Recommended Actions	Risk rating after mitigation			Status
			Likelihood	Consequence	Risk score		Likelihood	Consequence	Risk score	
	NHS number list emailed to the wrong recipient	No other information will be on the email, so the recipient will only have access to a list of NHS numbers.	2	2	4	A test email will be sent before the email including the NHS numbers are sent.	2	1	**2**	
	NHS number is accidentally shared on the call, rather than the pseudo-IDs	The people on the call would be able to identify the patient being discussed, and attribute their care/treatment to the NHS number.	2	2	4	All parties have been informed not to share any identifiable information, and this will be re-stated on the call.	2	1	**2**	

Risk Scoring Matrix.pdf

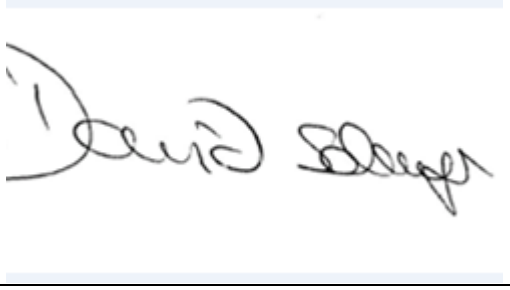
Step 9: Sign off - Divisional Information Assets Owner/Assistant

DIVISIONAL INFORMATION ASSETS OWNER/ASSISTANT

Notes IAO/IAA needs to confirm: - Is aware of the assessment, risks, processing, data flows - Adds any new system/equipment/processing on to the Divisional Information Assets Register and data flow mapping records post approval - Acknowledges that the DPIA needs to be reviewed if the nature, scope or purposes of the processing change.			
IAO/IAA NAME/SIGNATURE		DATE	4.8.22 – Lisa Gowan, Divisional General Manager

Step 10: Sign off and record outcomes – IG TEAM TO ACTION

CALDICOTT GUARDIAN/SIRO OPINION

APPROVED	☒	
CONDITIONALLY APPROVED (PENDING THE COMPLETION OF THE FOLLOWING ACTIONS)	☐	
REJECTED (FOR THE FOLLOWING REASONS)	☐	
CALDICOTT GUARDIAN NAME/SIGNATURE		
DATE	**3rd August 2022**	

DATA PROTECTION OFFICER (DPO)

DPO COMMENTS	

Notes

DPO needs to be satisfied that:

- Risks have been identified and adequately mitigated
- Any actions for conditional approved will be resolved
- The ICO is consulted where high risk processing is not mitigated
- DPIA is reviewed to ensure ongoing compliance.

If DPO decision departs from SIRO/Caldicott Guardian, DPO must explain what has been done to resolve any discrepancy.

DPO NAME/SIGNATURE	**Jacquie Widdowson**
DATE	**13th May 2022**