

National Record Locator – Data Protection Impact Assessment

Table of contents

Data protection impact assessment (DPIA).....	2
SECTION 1 – Screening questions	3
SECTION 2 – Why do you need the data?	4
SECTION 3 – What data do you want to use or share?	4
SECTION 4 – Where will data flow?	8
SECTION 5 – Is the intended use of the data lawful?.....	9
SECTION 6 – How are you keeping the data secure?.....	10
SECTION 7 – How long are you keeping the data and what will happen to it after that time?.....	11
SECTION 8 – How are people’s rights and choices being met?.....	12
SECTION 9 – Which organisations are involved?	14
SECTION 10 – What data protections are there and what mitigations will you put in place?	16
SECTION 11 – Review and sign-off	18

Data protection impact assessment (DPIA)

Data protection impact assessment (DPIA) title:	National Record Locator V.3.1
	NRL DPIA (Phase 2)
Date:	19 September 2023
Data Controller(s)	NRL Providers NRL Consumers NHS England (Limited controllership)

SECTION 1 – Screening questions

1. Do you need to do a DPIA?

Yes, the NRL involves large scale processing of personal data. Scope of data available through the NRL has widened and additional organisation types have been added as Providers and/or Consumers since the last DPIA was carried out.

a. Summary of how data will be used and shared

The NRL is an England wide index of pointers to confirm that a record is held for a patient. Organisations who use the NRL are called Providers and Consumers.

The Provider will publish 'Pointers' on the NRL via their Electronic Patient Record (EPR). The Pointer confirms that a Patient Record is available and the categories or type(s) of document. The Pointer includes a URL to retrieve the information (via the NHSE provisioned proxy authentication service) and/or the contact details of the Provider. Some Providers choose to upload their contact details only.

A Consumer can request access to a Patient Record from within the types of document(s) it is authorised to access, by clicking on the retrieval URL. The request to the Provider will include the Consumer's ODS code but does not identify the member of staff making the request.

The requested information is then collated by the Provider's EPR and sent via the proxy authentication service to the Consumer.

Consumers can request information from the NRL either via their EPR direct integration with the NRL or through the National Care

b. Description of the data

<input checked="" type="checkbox"/>	Personal data
<input type="checkbox"/>	Pseudonymised
<input type="checkbox"/>	Anonymous

SECTION 2 – Why do you need the data?

2. What are the purposes for using or sharing the data?

The purpose for sharing the data is to help staff from Consumer organisations to make informed decisions about direct care, including in emergency situations. It also assists Consumers (particularly ambulance staff) to prioritise resources more effectively. For example, the information may help paramedics assess whether to treat a patient at home or transport them to hospital. The below list includes some of the anticipated benefits that can be realised through sharing patient data through the NRL.

- Improved (mental) health outcomes
- Improved patient safety
- Improved staff safety
- Improving experience of health and care services
- Saving money by avoiding duplicate care
- Reducing healthcare usage
- Better provision of patient centred care
- Better able to meet patient care preferences

In addition, the NRL supports other NHSE programmes, including the ‘Data Saves Lives’ strategy.

3. What are the benefits of using or sharing the data?

- Information to inform decisions about the delivery of direct care.

SECTION 3 – What data do you want to use or share?

4. Can you use anonymous data for your purposes? If not, explain why.

<input type="checkbox"/>	Yes
<input checked="" type="checkbox"/>	No
<input type="checkbox"/>	Unsure

Personal data is needed for the delivery of direct care.

5. Which types of personal data do you need to use and why?

<input checked="" type="checkbox"/>	Forename	<input type="checkbox"/>	Physical description, for example height	<input type="checkbox"/>	Photograph / picture of people
<input checked="" type="checkbox"/>	Surname	<input type="checkbox"/>	Phone number	<input type="checkbox"/>	Location data e.g. <ul style="list-style-type: none"> • IP address

				<input type="checkbox"/>	• Other
<input checked="" type="checkbox"/>	Address	<input type="checkbox"/>	Email address	<input type="checkbox"/>	Audio recordings
<input checked="" type="checkbox"/>	Postcode full	<input type="checkbox"/>	GP details	<input type="checkbox"/>	Video recordings
<input type="checkbox"/>	Postcode partial	<input type="checkbox"/>	Legal representative name (personal representative)	<input type="checkbox"/>	Other
<input checked="" type="checkbox"/>	Date of birth	<input checked="" type="checkbox"/>	NHS number	<input type="checkbox"/>	None
<input checked="" type="checkbox"/>	Age	<input type="checkbox"/>	National insurance number		
<input checked="" type="checkbox"/>	Gender	<input type="checkbox"/>	Other numerical identifier		

To data is needed to identify the correct patient record. The data is also included on the documents that are retrieved.

- 6. Data protection laws mean that some data is considered particularly sensitive. This is called special category data. Data that relates to criminal offences is also considered particularly sensitive. Which types of sensitive data do you need to use or share?**

Type of data		Reason why this is needed (leave blank if not applicable)
<input checked="" type="checkbox"/>	Information relating to an individual's physical or mental health or condition, for example information from health and care records	Required for delivery of direct care
<input type="checkbox"/>	Biometric information in order to uniquely identify an individual, for example facial recognition	
<input type="checkbox"/>	Genetic data, for example details about a DNA sample taken as part of a genetic clinical service	
<input type="checkbox"/>	Information relating to an individual's sexual life or sexual orientation	

<input type="checkbox"/>	Racial or ethnic origin	
<input type="checkbox"/>	Political opinions	
<input type="checkbox"/>	Religious or philosophical beliefs	
<input type="checkbox"/>	Trade union membership	
<input type="checkbox"/>	Information relating to criminal or suspected criminal offences	
<input type="checkbox"/>	None of the above	

7. Who are the individuals that can be identified from the data?

<input checked="" type="checkbox"/>	Patients or service users
<input checked="" type="checkbox"/>	Carers (if named on care plan)
<input checked="" type="checkbox"/>	Staff (from care plan, if named at pointer)
<input type="checkbox"/>	Wider workforce
<input type="checkbox"/>	Visitors
<input type="checkbox"/>	Members of the public
<input type="checkbox"/>	Other

8. Where will your data come from?

Via published pointers added to the NRL by the Providers (the holders of the information). Current information types are care plans, NEWS2 reports, ambulance reports, Situation, Background, Assessment, Recommendation and Decision (SBARD) documents, shared care records.

Care plans are Mental health, Anticipatory, End of life, respect, urgent and emergency, integrated care and support, eRedBag.

9. Will you be linking any data together?

<input type="checkbox"/>	Yes
<input checked="" type="checkbox"/>	No
<input type="checkbox"/>	Unsure

a. Will it become possible, as a result of linking data, to be able to identify individuals who were not already identifiable from the original dataset?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No
<input type="checkbox"/>	Unsure

SECTION 4 – Where will data flow?

10. Describe the flows of data.

The NRL process is summarised below:

- a. The Provider will publish 'Pointers' on the NRL via their Electronic Patient Record (EPR). The Pointer confirms that there is an Appropriate Patient Record available for a patient. The Pointer includes a URL to retrieve the information via Spine Secure Proxy (SSP). Where selected by a Provider, it may also contain the contact details of the Provider.
- b. The Consumer can request access to the Appropriate Patient Record by clicking on the retrieval URL. The request to the Provider will include the Consumer's ODS code but does not identify the member of staff making the request.
- c. The requested information is then collated into a PDF by the Provider's EPR and sent (via the SSP) to the Consumer.
- d. Consumers can request information from the NRL either via their EPR direct integration with the NRL or through the National Care Records Service (NCRS).
- e. Organisations can be NRL Providers, NRL Consumers, or both.

11. Confirm that your organisation's information asset register (IAR), record of processing activities (ROPA) or your combined information assets and flows register (IAFR) has been updated with the flows described above.

Providers who are the originating data controllers for the data are required to include this processing in their Privacy Notices. Both Providers and Consumers are expected to include access to the NRL (where appropriate) in their business processes/data flows.

NRL is included on the NHSE Information Asset Register.

<input checked="" type="checkbox"/>	Yes
<input type="checkbox"/>	No
<input type="checkbox"/>	Unsure

12. Will any data be shared outside of the UK?

<input type="checkbox"/>	Yes
<input checked="" type="checkbox"/>	No
<input type="checkbox"/>	Unsure

a. If yes, give details, including any safeguards or measures put in place to protect the data whilst outside of the UK.

N/A

SECTION 5 – Is the intended use of the data lawful?

13. Under Article 6 of the UK General Data Protection Regulation (UK GDPR) what is your lawful basis for processing personal data?

<input type="checkbox"/>	(a) We have consent
<input type="checkbox"/>	(b) We have a contractual obligation
<input type="checkbox"/>	(c) We have a legal obligation
<input checked="" type="checkbox"/>	(e) We need it to perform a public task
<input type="checkbox"/>	(f) We have a legitimate interest
<input type="checkbox"/>	Other

14. If you have indicated in question 6 that you are using special category data, what is your lawful basis under Article 9 of the UK GDPR?

<input type="checkbox"/>	(b) We need it to comply with our legal obligations for employment
<input type="checkbox"/>	(f) We need it for legal claims, to seek legal advice or judicial acts
<input type="checkbox"/>	(g) We need to comply with our legal obligations to provide information where there is a substantial public interest , as set out in this list
<input checked="" type="checkbox"/>	(h) We need it to comply with our legal obligations to provide or manage health or social care
<input type="checkbox"/>	(i) We need it to comply with our legal obligations for public health
<input type="checkbox"/>	(j) We need it for archiving, research and statistics where this is in the public interest
<input type="checkbox"/>	Other
<input type="checkbox"/>	Not applicable

15. What is your legal basis for using and sharing this health and care data under the common law duty of confidentiality?

<input checked="" type="checkbox"/>	Implied consent
<input type="checkbox"/>	Explicit consent

<input type="checkbox"/>	Section 251 support
<input type="checkbox"/>	Legal requirement
<input type="checkbox"/>	Overriding public interest
<input type="checkbox"/>	Not applicable

a. Please provide further information or evidence.

Information is processed for the purpose of direct care.

SECTION 6 – How are you keeping the data secure?

16. Are you collecting information?

<input type="checkbox"/>	Yes [go to question 16a]
<input checked="" type="checkbox"/>	No [skip to question 17]

a. How is the data being collected?

17. Are you storing information?

<input checked="" type="checkbox"/>	Yes [go to question 17a]
<input type="checkbox"/>	No [skip to question 18]

a. How will information be stored?

[Put an next to all that apply.]

Storage location		Details (leave blank if not applicable)
<input type="checkbox"/>	Physical storage, for example filing cabinets, archive rooms etc	[provide details including whether the facility is operated by your organisation or a third party]
<input type="checkbox"/>	Local organisation servers	[provide details]
<input checked="" type="checkbox"/>	Cloud storage	NHSE only stores the Pointers. The only personal data included in the Pointer are the NHS Number and where relevant the key contact for the record (this is optional).
<input type="checkbox"/>	Other	[please state]

18. Are you transferring information?

<input type="checkbox"/>	Yes [go to question 18a]
<input checked="" type="checkbox"/>	No [skip to question 19]

a. How will information be transferred?

19. How will you ensure that information is safe and secure?

Security measure	Details (leave blank if not applicable)
<input type="checkbox"/> Encryption	
<input type="checkbox"/> Password protection	
<input checked="" type="checkbox"/> Role based access controls (RBAC)	RBAC is assigned by the end user organisation (Providers and Consumers) in line with their organisational Registration Authority Policy.
<input type="checkbox"/> Restricted physical access	
<input type="checkbox"/> Business continuity plans	
<input type="checkbox"/> Security policies	
<input type="checkbox"/> Other	

20. How will you ensure the information will not be used for any other purposes beyond those set out in [question 2](#)?

Specify the measures below which will be used to limit the purposes the data is used for.

Security measure	Details (leave blank if not applicable)
<input type="checkbox"/> Contract	
<input type="checkbox"/> Data processing agreement	
<input checked="" type="checkbox"/> Data sharing agreement	
<input type="checkbox"/> Data sharing and processing agreement (DSPA)	
<input checked="" type="checkbox"/> Audit	
<input type="checkbox"/> Staff training	
<input type="checkbox"/> Other	

SECTION 7 – How long are you keeping the data and what will happen to it after that time?

21. How long are you planning to use the data for?

N/A – NHSE does not directly use the data.

22. How long do you intend to keep the data?

Only pointers are held on the NRL. The Provider (holder of the information) is responsible for retention of the information.

23. What will happen to the data at the end of this period?

Action	Details (leave blank if not applicable)
<input type="checkbox"/> Secure destruction (for example by shredding paper records or wiping hard drives with evidence of a certificate of destruction)	
<input type="checkbox"/> Permanent preservation by transferring the data to a Place of Deposit run by the National Archives	
<input type="checkbox"/> Transfer to another organisation	
<input type="checkbox"/> Extension to retention period	
<input type="checkbox"/> It will be anonymised and kept	
<input checked="" type="checkbox"/> The controller(s) will manage as it is held by them	
<input type="checkbox"/> Other	

SECTION 8 – How are people’s rights and choices being met?

24. How will you comply with the following individual rights (where they apply)?

Individual right	How you will comply (or state <i>not applicable</i> if the right does not apply)
The right to be informed The right to be informed about the collection and use of personal data.	<input type="checkbox"/> Data controller privacy notice(s)
	<input checked="" type="checkbox"/> Privacy notice(s) for all relevant organisations
	<input type="checkbox"/> Information leaflets
	<input type="checkbox"/> Posters

	<input type="checkbox"/> Letters <input type="checkbox"/> Emails <input type="checkbox"/> Texts <input type="checkbox"/> Social media campaign <input type="checkbox"/> DPIA published (best practice rather than requirement) <input checked="" type="checkbox"/> Other: NHSE publicly available information on its website <input type="checkbox"/> Not applicable
The right of access The right to access details of data use and receive a copy of their personal information - this is commonly referred to as a subject access request.	Data Controller Privacy Notices Data Sharing Agreement
The right to rectification The right to have inaccurate personal data rectified or completed if it is incomplete.	Provider responsibility as originating data controller.
The right to erasure The right to have personal data erased, if applicable.	N/A
The right to restrict processing The right to limit how their data is used, if applicable.	N/A
The right to data portability The right to obtain and re-use their personal data, if applicable.	N/A
The right to object The right to object to the use and sharing of personal data, if applicable.	Provider and Consumer Privacy Notices should explain how patients can object to the processing of their data via the NRL. Objections are handled by the originating data controller.

25. Will the national data opt-out need to be applied?

<input type="checkbox"/>	Yes
<input checked="" type="checkbox"/>	No – processing is for direct care purposes
<input type="checkbox"/>	Unsure

26. Will any decisions be made in a purely automated way without any human involvement (automated decision making)?

<input type="checkbox"/>	Yes [go to question 26a]
<input checked="" type="checkbox"/>	No [skip to question 27]
<input type="checkbox"/>	Unsure [add as a risk in section 10 with an action to find out]

a. Where the effect of the automated decision on the individual is substantial, how will you uphold an individual’s right not to be subjected to a decision solely made by automated means)?

b. Are you using any special category data as part of automated decision making?

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

27. Detail any stakeholder consultation that has taken place (if applicable).

Stakeholder engagement takes place for each new use case.

SECTION 9 – Which organisations are involved?

28. List the organisation(s) that will decide why and how the data is being used and shared (controllers).

There are 100s of organisations who are Providers and/or Consumers. The list is not finite and remains subject to change as new organisations are added or removed from the NRL.

29. List the organisation(s) that are being instructed to use or share the data (processors).

The processors are Electronic Patient Record suppliers. As the NRL is an evolving services, the list is not finite and is constantly subject to change.

30. List any organisations that have been subcontracted by your processor to handle data

N/A

31. Explain the relationship between the organisations set out in [questions 28, 29](#) and [30](#) and what activities they do

The NRL is an England wide index of pointers to confirm that a record is held for a patient. Organisations who use the NRL are called Providers and Consumers.

Providers publish pointers on the NRL to confirm that they hold a record for the patient that can be accessed through the NRL by Consumers.

The pointer includes the patient NHS Number, what type of information is held, the Provider ODS code and name of setting, a URL to contact details (optional) and a URL to request access to it. Consumers can then request access to the information from the pointer.

Both Providers and Consumers are providers of direct care, and information on the NRL can only be accessed by Consumers for direct care purposes.

All organisations, including NHSE, are data controllers. NHSE's controllership is limited to the Pointers.

32. What due diligence measures and checks have been carried out on any processors used?

Due diligence measures		Details (leave blank if not applicable)
<input checked="" type="checkbox"/>	Data Security and Protection Toolkit (DSPT) compliance	
<input type="checkbox"/>	Registered with the Information Commissioner's Office (ICO)	

<input type="checkbox"/>	Digital Technology Assessment Criteria (DTAC) assessment	
<input type="checkbox"/>	Stated accreditations	
<input type="checkbox"/>	Cyber Essentials or any other cyber security certification	
<input checked="" type="checkbox"/>	Other checks	Supplier Connection Agreement Conformance documentation (SCAL)

SECTION 10 – What data protections are there and what mitigations will you put in place?

33. Complete the [risk assessment table](#). Use the [risk scoring table](#) to decide on the risk score.

Risk assessment table

Risk ref no.	Description	Risk score* (L x I)	Mitigations	Risk score* with mitigations applied
01	Confidentiality: Inadequate transparency materials to satisfy the data subject 'right to be informed' and 'right to object'.	8	<ul style="list-style-type: none"> Publish NHSE Privacy Notice on NRL website and include link in end user Data Sharing Agreement and/or NRL website. Remind end users to include the NRL in their own Privacy Notices. 	6
02	Confidentiality: Inconsistency in end user RBAC Controls for different staff roles.	5	<ul style="list-style-type: none"> User forums EPR supplier forums 	2
03	Availability: Individual end user pointers are inaccessible. This would impact on patient care, increasing risks of preventable clinical harm to patients, and increasing safeguarding risks. Lack of availability could be caused by:	16	<ul style="list-style-type: none"> Proactive audit programme to identify inactivity. NHSE to introduce an NRL dashboard and daily monitoring. This will diagnose whether an issue is with a particular Consumer/Provider, or whether it is 	12

	<ul style="list-style-type: none"> • Issues with the NRL service – e.g. network problems, issues following a new release • Issues with the NCRS (e.g. following a new release) • Issues with supplier systems • Lack of network signal for mobile NRL consumers (e.g. paramedics in ambulances) 		<p>system-wide, so that end users can be notified</p> <ul style="list-style-type: none"> • Encourage system suppliers to put active monitoring in place • Ambulance services are deploying satellite terminals on the roofs of ambulances to provide connectivity in areas where there is poor network coverage 	
04	Confidentiality and Availability: Lack of published audit programme and how audit data is disseminated to end users for their own audit purposes.	10	<ul style="list-style-type: none"> • Proactive and reactive audit programmes. • Audit data to be disseminated to end users and suppliers. . • Suppliers should also provide audit data to end users. 	6
05	Integrity and Availability: Supplier DSPT status not monitored or included in supplier connection agreement.	10	Add to supplier Connection Agreement.	0

***Risk scoring table**

		Impact (I)				
		Negligible (1)	Low (2)	Moderate (3)	Significant (4)	Catastrophic (5)
Likelihood (L)	Rare (1)	1	2	3	4	5
	Unlikely (2)	2	4	6	8	10
	Possible (3)	3	6	9	12	15
	Likely (4)	4	8	12	16	20
	Almost certain (5)	5	10	15	20	25

34. Detail any actions needed to mitigate any risks, who has approved the action, who owns the action, when it is due and whether it is complete.

Risk ref no.	Action needed	Action approver	Action owner	Due date	Status e.g. outstanding/complete
1	Create NRL NHSE Privacy Notice	Deputy Delivery Director: Clinical Data Sharing Lead Platforms/Clinical Pillar	Programmes Information Governance (IG) Lead	13 Oct 2023	Outstanding
2	Share RBAC controls at supplier and end user forums	Deputy Delivery Director: Clinical Data Sharing Lead Platforms/ Clinical Pillar	NRL Implementation Specialist	31 October 2023	Outstanding
3	System audits	Service Manager NRL	NRL Service Manager	31 October 2023	Outstanding
4	Published audits	Deputy Delivery Director: Clinical Data Sharing Lead Platforms/Clinical Pillar		31 December 2023	Outstanding
5	Supplier DSPT status i) Add requirement to supplier connection agreement ii) monitor DSPT improvement plans for suppliers and end users where status below 'Standards met'	Deputy Delivery Director: Clinical Data Sharing Lead Platforms/ Clinical Pillar	i) Programmes IG lead ii) NRL Service Manager	13 October 2023	Outstanding

SECTION 11 – Review and sign-off

Reviewer sign-off	
Reviewer name:	
Reviewer job title:	

Reviewer contact details:	NRL Implementation specialist
Date of review:	
Comments:	
Date for next review:	7 December 2023

Approver sign-off	
Approver name:	(Redacted)
Approver job title:	Deputy Delivery Director: Clinical Data Sharing Lead Platforms/Clinical Pillar
Date of approval:	19 September 2023
Comments:	