Data Protection Impact Assessment for the National Neonatal Audit Programme (England, Scotland, Wales and the Isle of Man)

Document control:

	Name and role	Contact details
Document Completed by	Rachel Winch, NNAP Project Manager	rachel.winch@rcpch.ac.uk 020 3861 1910
Data Protection Officer name	Adele Picken, Head of Information Governance	Adele.Picken@rcpch.ac.uk 020 7092 6030
Document approved by (this should not be the same person that completes the form).	Adele Picken, Head of Information Governance	Adele.Picken@rcpch.ac.uk 020 7092 6030
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	Z5143673	

Date Completed	Version	Summary of changes
23/11/2020	0.1	Draft as part of PIA meeting- following change to data flow
26/11/2020	0.2	JE edits to draft
27/11/2020	0.3	Further edits to draft by RCPCH Head of IG
04/12/2020	0.4	Update following CAG application and verification of storage
01/03/2021	0.5	Update following confirmation of section 251 approval and HSC-PBPP application
01/04/2021	0.6	Review by Head of Information Governance, RCPCH and further updates by RW in consultation with IS team.
01/04/2021	1.0	Head of Information Governance final review and sign off
28/03/2022	1.1	Annual review by NNAP PM Rachel Winch, to incorporate Scottish data flow and amendments to English and Welsh data flow under Section 251.
04/07/2022	1.2	Review and amendments by Rachel Winch (NNAP PM), and Adele Picken (Head of Information Governance).
01/08/2022	1.3	Amendments by Rachel Winch (NNAP PM) following HSC-PBPP feedback, with review by Adele Picken (Head of Information Governance).
15/12/2023	1.4	Annual review by NNAP PM Rachel Winch. Updated to reflect exemption to National Data Opt Out (NDOO), proposed flow to data to UKHSA and linkage to SGSS by UKHSA, the introduction of a

		Microsoft PowerBI data dashboard to share open and restricted access reporting, addition of the Isle of Man, and retrospective Scottish data.
March 2025	1.5	Review by NNAP PM Rachel Winch and Adele Picken, Head of Information Governance.

Contents

Screening questions

Please complete the following checklist:

	Section	Yes or No	N/A	Comments
1.	Does your project involve any automated decision making, evaluation or scoring including profiling and predicting using information about a person? Does the outcome from your project decide who gets access to services?	N		
2	Does your project involve any sensitive information or information of a highly personal nature?	Y		
3.	Does the proposal involve any data concerning vulnerable individuals who may be unable to easily consent or oppose the processing, or exercise their rights? This group may include children, employees, mentally ill persons, asylum seekers, or the elderly, patients and cases where there is an imbalance in the relationship between the position of the individual and the controller.	Y		
4.	Does your project involve any innovative use or applying new technological or organisational solutions? This could include biometric or genetic data, the tracking of individuals' location or behaviour?	N		
5.	Does your project match data or combine datasets from different sources?	Y		
6.	Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	N		
7.	Does your project process data that might endanger the individual's physical health or safety in the event of a security breach?	Y		
8.	Is this a new project? Or have the requirements for your project changed since its initiation? Are you sharing new information or linking to new datasets that were not part of the original project specification. Have you added any new audit streams to your project?	Y		Existing project with linkage to a new dataset.

Data Protection Impact Assessment

This Data Protection Impact Assessment (DPIA) template and guide is a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. This tool will help organisations which process personal data to properly consider and address the privacy risk that this entails.

DPIA can be used alongside existing project management and risk management methodologies.

Conducting a DPIA is now a legal requirement under the GDPR (General Data Protection Regulation) which will start on the 25th May 2018 and the new UK Data Protection Act. By completing a DPIA, this will help to ensure that your project is compliant with GDPR and UK data protection legislation. This document will be updated if further ICO guidance is published or there is change in legislation.

A DPIA is the basis of a "privacy by design" approach, to help meet privacy and data protection expectations of customers, employees and other stakeholders. A DPIA is intended to be prospective and proactive and should act as an early warning system by considering privacy and compliance risks in the initial design and throughout the project.

Purpose and benefits of completing a DPIA

- A DPIA is a process which assists organisations in identifying and minimising the privacy risks of new projects or policies.
- Conducting a DPIA involves working with people within the organisation, with partner organisations and with the people affected to identify and reduce privacy risks.
- The DPIA will help determine the appropriate controls needed to protect personal data i.e. technical, procedural and physical.
- The DPIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Conducting a DPIA should benefit organisations by producing better policies and systems and improving the relationship between organisations and individuals.
- The ICO may often ask an organisation whether they have carried out a DPIA. It is often the most effective way to demonstrate to the ICO how personal data processing complies with Data Protection legislation.

Supplementary guidance

- Data Protection Impact Assessment under GDPR guidance
- ICO's conducting privacy impact assessments code of practice
- The ICO's Anonymisation: managing data protection risk code of practice may help organisations to identify privacy risks associated with the use of anonymised personal data.
- The ICO's Data sharing code of practice may help organisations to identify privacy risks associated with sharing personal data with other organisations.
- The ICO's codes of practice on privacy notices, as well as other more specific guidance, will also help an organisation to focus DPIAs on those issues.
- The Government Data Programme has developed a Data Science Ethical Framework to help organisations understand the benefits and risks of using personal data when developing policy. The

Framework can be used as part of the process to help you describe information flows and identify privacy risks and solutions.

DPIA methodology and project information.

At what stage in the project did you conduct this DPIA? E.g. planning stage, changes to the existing project, in retrospect.

Upon changing the data flow to require the RCPCH to hold section 251 approval to receive data for England and Wales, HSC-PBPP approval to receive data for Scotland. Upon changes to the existing project to incorporate linkage with the Second-Generation Surveillance System (SGSS) hosted by the UK Health Security Agency (UKHSA) (**pending awaiting information sharing agreement)**, the introduction of a Microsoft PowerBI data dashboard to share open and restricted access reporting, the expansion of the geographical coverage of the audit to include the Isle of Man, and on application for retrospective Scottish data (from 1 July 2017).

Describe the overall aim of the project and the data processing you carry out

The NNAP assesses whether babies admitted to neonatal units in England, Scotland, Wales and Isle of Man receive consistent high-quality care. We identify areas for quality improvement in relation to the delivery and outcomes of care.

DPIA Consultation

We advise you to consult with as many relevant people as possible (both internal and external stakeholders**)** while conducting this assessment, consultation is an important part of a DPIA and allows people to highlight privacy risks and solutions based on their own area of interest or expertise. Consultation can take place at any point in the DPIA process and may include the project management team, Data Protection Officer, designers, IT provider, procurement team, data processors, communications team, patients, stakeholders, corporate governance and compliance teams, researchers, analysts, statisticians and senior management.

You must consult with the Data Protection Officer regarding the impacts on privacy. Please state below that you have.

If you decide against seeking the views of data subjects or their representatives e.g. this would be disproportionate or impracticable, then the justification must be made clear in the box below. In the box below name the stakeholder group, date consulted and how consulted. Please insert another box if you consulted with many different stakeholder groups.

Key neonatal clinical professions and specialties are involved in the design and delivery of the NNAP via their representation on the NNAP M&DG and Board.

The NNAP Project Board is comprised of representatives nominated by key stakeholder organisations, including BAPM, Bliss, Neonatal Networks, Neonatal Critical Care CRG, Neonatal Nurses Association and the Neonatal Society as well as parent, neonatal trainee and regional clinical representatives.

The NNAP Project Board are consulted and kept informed about all changes to the design and delivery of the NNAP, and risks and issues are reported to the Board on a quarterly basis.

A focus group of parents with experience of neonatal care, and individuals who experienced neonatal care as infants, was held in collaboration with Bliss to consult on the NNAP application for exemption from the National Data Opt Out in England. The application for exemption was made at the request of the NNAP M&DG and Board, and was supported by feedback from the focus group.

The NNAP consults with a parent representatives, neonatal nurses and network representatives to ensure that the information it provides for parents is fit for purpose and communicated in the most appropriate way. As a result of feedback from these representatives and from the Confidentiality Advisory Group (CAG) at the Health Research Authority (HRA), the NNAP have restructured it's privacy notice and developed a short animation which links to further detail.

The NNAP M&DG and Board have been involved in the design of the PowerBI data dashboard, and the data dashboard has been reviewed by a multidisciplinary stakeholder group.

To further enhance opportunities to seek the views of data subjects and their representatives, the NNAP have established a Parent Partnership Group (PPG).

Publishing your DPIA report

Publishing a DPIA report is not a legal requirement but you should consider publishing this report (or a summary or a conclusion) and you should send it to your stakeholders. Publishing the DPIA report will improve transparency and accountability, and lets individuals know more about how your project affects them. Though there may be a need to redact/remove sensitive elements e.g. information on security measures.

State in the box below if you are going to publish your DPIA. If so, please provide hyperlink to the relevant webpage if this has been done already or insert the date you intend to publish it.

Published on the NNAP pages of the RCPCH website, at: https://www.rcpch.ac.uk/resources/national-neonatal-audit-programme-transparency-open-data

Please describe how personal information is collected, stored, used and deleted. Use your data flow map and information asset register to help complete this section. Explain what personal information is used, what it is used for, who it is obtained from and disclosed to, who will have access and any other necessary information. Completing this section can help identify potential ‘function creep’, unforeseen or unintended uses of the data for example data sharing. Please see NNAP data flow map: https://www.rcpch.ac.uk/work-we-do/clinical-audits/nnap/data-flow#data-flow-in-the-nnap

Processing activity description	**Type of data involved**	**Data flow**	**Controller/processor**
Clinical data entered by neonatal units on BadgerNet system	Personal and Special Category data (identifiable)	Neonatal unit to System C.	Data controller: NHS Trust/Health Board Data Processor: System C
Clinical data stored by System C on BadgerNet system	Personal data and Special Category (identifiable)	None.	Data processor: System C Data controller: NHS Trust/Health Board
Neonatal Dataset SQL Database created within the System C Microsoft Azure environment containing full neonatal dataset extracted from BadgerNet (not accessible by RCPCH)	Personal data and Special Category (identifiable)	None.	Data processor: System C Data controller: NHS Trust/Health Board
NNAP Database synchronised to a 'mirror' NNAP SQL server database on RCPCH Azure hosting infrastructure	Personal data and Special Category (identifiable)	System C to RCPCH	Data processor: RCPCH Data controller: HQIP
Pending: Subset of NNAP dataset sent to UKHSA linkage with SGSS data (English data only).	Personal data and Special Category (identifiable)	RCPCH to UKHSA	Data processors: RCPCH, UKHSA Data controllers: HQIP/NHSE, UKHSA
Pending: Pseudonymised, linked NNAP-SGSS data sent to RCPCH (English data only).	Pseudonymised, sensitive	UKHSA to RCPCH	Data processors: RCPCH, UKHSA Data controllers: HQIP/NHSE, UKHSA
Quarterly or monthly neonatal unit reports shared with neonatal unit and respective networks only. Data quality and completeness episode lists shared with neonatal units responsible for the data. Shared via PowerBI data dashboard (restricted access)	Anonymised, aggregated, small number masking not applied. Episode lists – Pseudonymised - BadgerNet ID (hospital identifier) only, no other patient identifiable information.	RCPCH to neonatal units and networks	Data processor: RCPCH Data controller: HQIP/NHS England (for English data)/ Digital Health and Care Wales (for Welsh data)
Re-extracted, cleaned data used to develop tables and statistical outputs for NNAP reporting, including PowerBI data dashboard (open access).	Pseudonymised/ limited access deidentified becomes anonymised and aggregated data (non-identifiable)	RCPCH	Data processor: RCPCH Data controller: HQIP/NHS England (for English data)/ Digital Health and Care Wales (for Welsh data)

If NNAP data is linked or onward shared (not applicable to Scotland, no onward sharing)			
(England) *If* NNAP data is to be linked or shared, the RCPCH send list of NHS numbers to NHSD for national opt out programme check	Personal data and Special Category (identifiable)	RCPCH to NHS Digital	Data processor: RCPCH Data controller: NHS Digital Data controller: HQIP

(England) NHSD send list of NHS numbers to RCPCH, removing any that have opted out under the national opt out	Personal data and Special Category (identifiable)	NHS Digital to the RCPCH	Data processor: RCPCH Data controller: NHS Digital Data controller: HQIP
(England) Opt outs removed and data cleaned.	Personal data and Special Category (identifiable)	None.	Data processor: RCPCH Data controller: HQIP

Transferring personal data outside the European Economic Area (EEA)

If personal data is being transferred outside of the EEA, describe how the data will be adequately protected (e.g. the recipient is in a country which is listed on the Information Commissioner's list of "approved" countries, or how the data is adequately protected).

Not applicable – data will not be transferred outside of the EEA.

Justification for collecting personal data

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. In certain circumstances it may be unlawful to process information not described in the transparency information (privacy notice/fair processing material) which informs individuals how their personal data is being used.

It may not be necessary to process certain data items to achieve the purpose. They may be irrelevant or excessive leading to risk of non-compliance with the Data Protection Act.

In the tables below list and justify personal data items needed to achieve the lawful aim of a project that requires information on individuals and their personal characteristics. Insert as many more lines that you need. Work through the table of items and decide whether or not you should be collecting the information, examine each data field and decide if you need it.

There are two sections in the table below, one for personal data and one for personal sensitive data items.

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Personal Data			
Name	N		
NHS number/CHI number	Y		BABY - Used as a baby's unique national identifier in a neonatal episode and will allow the RCPCH to de-duplicate the NNAP dataset, linking care episodes for a baby that may occur in multiple neonatal units and follow up care provided in other hospitals. MOTHER - Used as a mother's unique national identifier and ensures that twins, triplets and other multiple births can be identified as associated with a single mother which is important for certain NNAP audit measures.
Address	N		
Postcode	Y		Used to establish LSOA deciles (DataZone & SIMD in Scotland) derived through the postcodes so that deprivation will form one of the background matching variables when estimating treatment effect for the NNAP mortality reporting measure.
Date of birth	Y		MOTHER - Used as one of the background matching variables when estimating treatment effect for the NNAP mortality reporting measure.

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
			BABY - Used as part of the criteria to derive the analysis for NNAP audit measures which have time-bound elements where the time between admission and delivery of the care process forms part of the success criteria, an example being “Does an admitted baby born at less than 32 weeks gestational age have a first temperature on admission which is both between 36.5–37.5°C and measured within one hour of birth?”.
Date of death	Y		BABY - Used as part of the criteria to derive the analysis for the Mortality to discharge in very preterm babies audit measure which asks, “Does a baby born at less than 32 weeks gestational age die before discharge home, or 44 weeks post-menstrual age (whichever occurs sooner)?”.
Age	Y		MOTHER – Calculated from date of birth. Used as one of the background matching variables when estimating treatment effect for the NNAP mortality reporting measure.
Sex	Y		Used as one of the background matching variables when estimating treatment effect for the NNAP mortality reporting measure.
Marital Status	N		
Gender	Y		Used as one of the background matching variables when estimating treatment effect for the NNAP mortality reporting measure.
Living Habits	Y		Smoking status for matching analysis
Professional Training / Awards	N		
Income / Financial / Tax Situation	N		
Email Address	N		
Physical Description	N		
General Identifier e.g. Hospital No	Y		Unique GUID to identify a single neonatal admission for an infant. The infant's EntityID is used to connect admission and demographic details to daily summary forms and other ad-hoc events recorded in relation to the infant (Rop Screenings, Sepsis screening, Developmental data, etc.).
Home Phone Number	N		
Online Identifier e.g. IP Address/Event Logs	N		
Website Cookies	N		
Mobile Phone / Device No	N		
Device Mobile Phone / Device IMEI	N		

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
No			
Location Data (Travel / GPS / GSM Data)	N		
Device MAC Address (Wireless Network Interface)	N		
Sensitive Personal Data			
Physical / Mental Health or Condition	Y		Of mother and baby. Used to compare outcomes for babies.
Sexual Life / Orientation	N		
Family / Lifestyle / Social Circumstance	Y		Smoking status or previous pregnancies, or index of deprivation (linked to postcode) for analysis.
Offences Committed / Alleged to have Committed	N		
Criminal Proceedings / Outcomes / Sentence	N		
Education / Professional Training	N		
Employment / Career History	N		
Financial Affairs	N		
Religion or Other Beliefs	N		
Trade Union membership	N		
Racial / Ethnic Origin	Y		Used as one of the background matching variables when estimating treatment effect for the NNAP mortality reporting measure.
Biometric Data (Fingerprints / Facial Recognition)	N		
Genetic Data	N		
Medical Treatment	Y		Required for analyses (steroids, magnesium sulphate etc)

Data quality standards for personal data

In the box below, describe how you will ensure that personal data is accurate and kept up to date.

The RCPCH receive a live sync of a subset of the data stored on the BadgerNet system run by System C. This means that the RCPCH has access to the most up to date version of the data, and any changes or corrections made to the patient record are reflected in the NNAP live data sync.

Versions of the identifiable data will be saved on the Azure server at regular (quarterly or monthly) intervals with version controls applied. The identifiable data will not be copied and stored anywhere else, apart from the back up. Pseudonymised versions of the database will be saved on the RCPCH Microsoft Azure server at regular (quarterly or monthly) intervals for analysis at a given snapshot in time.

The NNAP team issues quarterly or monthly data quality and completeness reports to Health Boards/Trusts so that they can review and correct their data. Changes made are reflected in their next report via the live data sync.

Individual's rights

If your project uses personal data you must complete this section.

If your project uses personal data you must state how fairness and transparency will be achieved e.g. privacy notices on websites, posters, and leaflets. The information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Any information provided to children should be in such a clear and plain language that the child / vulnerable person can easily understand.

In the box below, please define the way you have ensured that individuals are aware of the rights, if they request those rights how will they achieve them? For example if an individual requests a copy of their information held by you, describe how you would do this. You can insert any relevant policy or process guides in the appendix at the end of this document if they are not already available on your website. This section does not refer to the personal information held about your audit staff.

Please see NNAP parent information leaflet: https://www.rcpch.ac.uk/resources/national-neonatal-audit-programme-your-babys-information

Individuals rights (where relevant)	**Describe how you ensure individuals are aware of these rights**	**Describe how you would do this**	**Please copy and paste section of document that states the individuals rights**
Individuals are clear about how their personal data is being used.	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units.	Not applicable.
Individuals can access information held about them	Included in the privacy notice.	If a parent makes an SAR on behalf of their child to NNAP we will forward this onto the Trust/Health Board providing their care. We have a specific procedure for dealing with rights requests in relation to clinical audits and this will be followed.	The personal data we hold about you is provided by your unit. We can let you know which categories of data we collect but you will need to contact your unit directly for a copy of your personal data as they are data controllers of your patient record.
Request erasure (right to be forgotten) in certain circumstances, making clear that it does not apply to an individual's health or care record, or for public health or scientific research purposes	Included in the privacy notice.	As the data is being processed for a public interest, this right does not apply. If we receive a request, we will respond to this affect. Any requests relating directly to the patient record will be forwarded to the Trust/ Health Board. We have a specific procedure for dealing	The right of erasure does not apply to this audit because your data is being processed for the purposes of performing a task in the public interest, which in this case is for ensuring high standards of quality and safety health care. However, if you want to opt out of future audit rounds, please let your unit know and they will remove you from the submission so that we don't receive the data. **<u>Isle of Man</u>**

		with rights requests in relation to clinical audits and this is outlined in this procedure.	The right of erasure does not apply to this audit because your data is being processed for the purposes of performing a task in the public interest, which in this case is for ensuring high standards of quality and safety health care. However, if you want to opt out of future audit rounds, please contact fps@gov.im and they will remove you from the submission so that we don't receive the data.
Rectification of inaccurate information	Included in the privacy notice.	Forward the request to the Health Board/Trust who are data controller of the patient record. We have a specific procedure for dealing with rights requests in relation to clinical audits and this will be followed.	Any requests to amend or update your personal data should be sent to your NHS Trust/Health Board as data controller. If we receive any requests, we will forward these to the unit.
Restriction of some processing	Included in the privacy notice.	Forward the request to the Trust /Health Board who are the data controller of the patient record. We have a specific procedure for dealing with rights requests in relation to clinical audits and this will be followed.	Any requests for restriction of processing should be sent to your NHS Trust/Health Board and they will inform us where applicable.
Object to processing undertaken on some legal bases	Included in the privacy notice.	Forward the request to the Trust/ Health Board who are the data controller of the patient record.	**Right to Erasure and Right to Object** **Scotland:** The right of erasure does not apply to this audit because your data is being processed for the purposes of performing a task in the public interest, which in this case is for ensuring high standards of quality and safety health care. However, if you do not want your personal data to be used for future rounds of the NNAP, please let your neonatal unit know and they will remove you from the submission so that we don't receive the data. The Health Board providing your neonatal care will still retain your overall healthcare data.

			England and Wales: The National Data Opt Out (which allows patients in England to opt out of their information being used for purposes beyond their direct care) does not apply to the National Neonatal Audit Programme. This is because applying the National Data Opt Out would introduce biases to the data and jeopardise patient safety. **You can still choose for your baby's information not to be used for the purpose of the NNAP, more details on how you can do this are provided below in the *Do you ask my permission to use my baby's information?* section.** **Isle of Man:** The right of erasure does not apply to this audit because your data is being processed for the purposes of performing a task in the public interest, which in this case is for ensuring high standards of quality and safety health care. However, if you want to opt out of future audit rounds, please contact fps@gov.im and they will remove you from the submission so that we don't receive the data.
Complain to the Information Commissioner's Office;	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units. Individual can contact the ICO directly with a complaint via the email provided on our privacy notice to them.	England and Wales: You do also have the right to lodge a complaint with the Information Commissioner's Office (ICO) at casework@ico.org.uk if you have concerns about the way your baby's personal data are being handled. Scotland: You do also have the right to lodge a complaint with the Information Commissioner's Office (ICO) – Scotland at Scotland@ico.org.uk if you have concerns about the way your baby's personal data are being handled. Isle of Man: You do have the right to lodge a complaint with the UK Information Commissioner's Office (ICO) at casework@ico.org.uk if you have concerns about the way your

			baby’s personal data are being handled. You can also lodge a complaint with the Isle of Man Information Commissioner’s Office (ICO). For more information, please see their website: https://www.inforights.im/complaint-handling/how-to-make-a-complaint-to-the-information-commissioner/data-protection-complaints/.
Withdraw consent at any time (if processing is based on consent)	Not applicable.	Not applicable.	Not applicable.
Data portability (if relevant)	Not applicable.	Not applicable. Data is not collected directly from the data subject, part of a contract or based on consent.	Not applicable.
Individual knows the identity and contact details of the data controller and the data controllers data protection officer	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units.	Healthcare Quality Improvement Partnership (HQIP) is the data controller of the National Neonatal Audit Programme (jointly with NHS England for English data and Digital Health and Care Wales for Welsh data) and can also be contacted if you have any questions about how your information is being used for the audit. Please direct any queries for the Healthcare Quality Improvement Partnership Data Protection Officer to: communications@hqip.org.uk.
In which countries the data controller is processing their personal data. For data transfers outside the EU, a description of how the data will protected (e.g. the recipient is in an ‘adequate’ country / how a copy of the safeguards can be obtained.	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units.	Scotland: The NNAP does not share identifiable or pseudonymised data from Scottish services with others. Personal data shall not be transferred to a country or territory outside the UK unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. England, Wales: Data will only ever be shared with the approval of HQIP. For HQIP to approve the request, the requestor must be able to demonstrate compliance with stringent data

			protection policies and arrangements and the aims of the research must be approved, as per HQIP's guidance to applicants. Personal data shall not be transferred to a country or territory outside the UK unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. No individual babies are identified in any of our reports. Isle of Man: Manx Care will share your personal data with the NNAP audit which is based in the UK. As the UK is deemed adequate by the EU, they are also deemed adequate by the Isle of Man, so no further steps are required to ensure the transfer of your data from the Isle of Man to the UK. This is because the UK is considered to have equivalent data protection legislation in place which will provide the same level of protection to your data as it would receive in the Isle of Man. Data will only ever be further shared with the approval of HQIP. For HQIP to approve the request, the requestor must be able to demonstrate compliance with stringent data protection policies and arrangements and the aims of the research must be approved, as per HQIP's guidance to applicants.
To know the legal basis under which their information is processed. Is there a clear legal basis for the processing of personal data? If so, what is the legal basis?	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units. We are processing under schedule 6(e) and schedule 9(i) of UK GDPR.	Processing is permitted under the UK General Data Protection Regulation (UK GDPR) on the following legal bases: • Article 6 (1) (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This is justified through commissioning arrangements which link back to NHS England and the Welsh Government. • Article 9 (2) (i) processing is necessary for reasons of public

			interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy. This is justified as the NNAP aims to drive improvements in the quality and safety of care and to improve outcomes for patients. We also protect your privacy rights by providing you with the ability to choose for your data to not be included in the audit. Isle of Man: The NNAP data sharing has been approved by the Isle of Man Department of Health and Social Care and the Isle of Man Information Commissioner. Processing is permitted under the Isle of Man GDPR and LED Regulations 2018 on the following legal bases: • Applied GDPR Article 6 (1) (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, inter alia, Manx Care. • Applied GDPR Article 9(2)(h) processing is necessary for the purposes of ... the management of health or social care systems and services on the basis of Union law (as applied to the Island by or under the authority of an Act of Tynwald) or Manx law... and under Schedule 2, Regulation 12, Part 2(2)(f) the management of health care systems or services or social care systems or services...of the GDPR and LED Implementing Regulations 2018 to fulfil the statutory obligation placed upon Manx Care, prescribed under Section 23 of the Manx Care Act 2021

			namely, as to improvement in quality of services. • Public interest under the common law duty of confidentiality, reinforced by the Manx Care Act and the NHS Act 2001 which mandate Manx Care to provide the function around improvement of health and social care on behalf of the Isle of Man Dept. of Health and Social Care.
To know the purpose(s) for the processing of their information.	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units.	We use information about your baby's care to help neonatal units in England, Wales and Scotland to improve the care and outcomes for other babies.
Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the personal data.	Not applicable	Not applicable- there is no statutory obligation for parents to provide their baby's data to the NNAP audit.	Not applicable
The source of the data (where the data were not collected from the data subject)	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units.	Neonatal unit staff enter your baby's information onto a secure electronic record system named BadgerNet. All neonatal units share information from these electronic records with the National Neonatal Audit Programme (NNAP) project team within the RCPCH, via another processor, System C, who manage the BadgerNet system used by neonatal units to record clinical data.
Categories of data being processed	Included in the privacy notice. Data dictionary.	Published on our website, distributed electronically to neonatal units. Full data dictionary published on our website.	This includes sensitive personal data, including NHS or CHI Number (Baby and Mother), Date and time of admission to neonatal care (Baby), Date and time of discharge from neonatal care (Baby), Date and time of birth (Baby), Date of death (Baby), Date of birth (Mother), Ethnicity (Mother), Gender (Baby), Postcode of usual address (Mother) and information about the care that mum and baby received and any related health conditions. The NNAP project team only uses the information for the purpose of the National Neonatal Audit Programme to monitor and try to improve standards of patient care.
Recipients or categories of recipients	Included in the privacy notice.	The College may receive data access requests. (England and Wales) Any requests	England, Wales and Isle of Man: Data will only ever be shared with the approval of HQIP. For HQIP to approve the request, the requestor

		to access data will require a completed DARs request form. For Scotland, no identifiable or pseudonymised data will be shared.	must be able to demonstrate compliance with stringent data protection policies and arrangements and the aims of the research must be approved, as per HQIP's guidance to applicants. Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Scotland: The NNAP publishes data in anonymised, aggregated form. No individual babies are identified in any of our reports. The NNAP does not share identifiable or pseudonymised data from Scottish services with others.
The source of the personal data	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units.	Neonatal unit staff enter your baby's information onto a secure system for electronic records. All neonatal units share information from these electronic records with RCPCH.
To know the period for which their data will be stored (or the criteria used to determine that period)	Included in the privacy notice.	Published on our website, distributed electronically to neonatal units.	The NNAP team at the RCPCH acts as the data processor on behalf of HQIP, who are the data controllers for the NNAP data. HQIP are joint data controllers with NHS England for English NNAP data and with Digital Health and Care Wales (DHCW) for Welsh NNAP data. The RCPCH will hold the NNAP data for as long as it is contracted to deliver the NNAP. All patient identifiable data will be deleted at the end of our contract. If HQIP commissions the RCPCH to deliver the NNAP under a new or extended contract, then the data will be retained by the RCPCH for the period of the new contract.
The existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects (if applicable)	Not applicable.	Not applicable.	Not applicable.

Privacy Risks

Types of Privacy risks

- Risks affecting individuals or other third parties, for example; misuse or overuse of their personal data, loss of anonymity, intrusion into private life through monitoring activities, lack of transparency.
- Compliance risks e.g. breach of the GDPR
- Corporate risks (to the organisation), for example; failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of patients or the public.

Risks affecting individuals

Patients have an expectation that their privacy and confidentiality will be respected at all times, during their care and beyond. It is essential that the impact of the collection, use and disclosure of any patient information is considered in regards to the individual's privacy.

In the box below insert the number of individuals likely to be affected by the project. This could be the number of unique patient records your project holds now and how many more records you anticipate receiving each year.

Each year, the NNAP receives information about approximately 100,000 babies, with annual fluctuations.

Please complete the table below with all the potential risks to the Individuals of the information you hold on them, your corporate risks and compliance risks.

When completing the table you need to consider if:

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Corporate and compliance risks

In the table, list the corporate risks to your organisation which could include reputational damage, loss of public trust, financial costs and data breaches. Below these, insert any compliance risks.

Possible corporate risks include:

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Examples of compliance risks include:

- Non-compliance with the common law duty of confidentiality
- Non-compliance with the GDPR.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.

Managing Privacy and Related risks

There are many different steps you can take to reduce a privacy risk. For example

- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors that will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Use your project plan and a detailed explanation of information flows to identify more precisely how a general risk may occur. For example, there may be particular points in a process where accidental disclosure is more likely to happen.

The DPIA actions should be added to into your project plan and risks added to your contract review documentation.

Privacy Risks and Actions Table

Programme and Corporate/Commercial risk logs are held internally.