Data Protection Impact Assessment for Barts Health NHS Trust

National Institute for Cardiovascular Outcomes Research (NICOR)

Version 2 (Updated 21 October 2020)

Document control:

	Name and role	Contact details
Document Completed by	**James Chal NICOR Chief Operating Officer, Barts Health NHS Trust.**	**j.chal@nhs.net**
Data Protection Officer name	**Sarah Palmer-Edwards c/o Data Protection Officer, Barts Health NHS Trust**	DPO.bartshealth@nhs.net
Document approved by (this should not be the same person that completes the form).	**Sarah Palmer-Edwards c/o Data Protection Officer, Barts Health NHS Trust**	DPO.bartshealth@nhs.net
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	**Z3086438**	

Date Completed	Version	Summary of changes
19TH April 2018	**1.0 (draft)**	**Initial draft version**
30th April 2018	**1.0**	**Incorporated changes following review by Trusts Information Governance Manager**
5th October 2020	**2.0**	**Updated to include GDPR, to address PBPP queries raised by PBPP (for hospitals in Scotland) and feedback by Barts Health DPO.**
21 October 2020	**2.0**	**Approved by Barts Health NHS Trust DPO**

NICOR DPIA Version 2.0 approved by Sarah Palmer-Edwards, Head of Information Governance/DPO Barts Health NHS Trust	**Signature** **SE PALMER-EDWARDS**	**Date** **30 October 2020**

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/A	
2	Does your project involve any sensitive information or information of a highly personal nature?	Yes		The project collects personal information on patients who are treated for a number of cardiac conditions
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.	Yes		Individuals under-going emergency treatment and children being treated for congenital heart conditions
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/A	
5.	Does your project match data or combine datasets from different sources?	Yes		We link NCAP data with ONS civil registrations (mortality) and HES data in England and PEDW data from Wales for audit purposes. For England and Wales we also have CAG approval for performing these linkages for research purposes– so we anticipate performing these linkages once we have a DSA with NHS Digital. Once approved we anticipate linkages with mortality data and hospital episode statistics from Scotland to work out

				outcomes and co-morbidities.
6.	Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	No		The data is collected from patients by hospitals who are responsible for providing their own privacy notice
7.	Does your project process data that might endanger the individual's physical health or safety in the event of a security breach?	No		
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?	No		The National Clinical (Cardiac) Audits have been conducted for nearly two decades (and in Scotland for 15 years). However, this is the first time that we will have central approval (PBPP) for linking NCAP data with mortality data for calculating treatment outcomes. We would also like to link the (NCAP) data with hospitalisation data to work out other co-morbidities. In future we are intending to link NCAP data to other national clinical datasets e.g. the National Cardiac Rehabilitation Audit and Primary care data.

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 General Data Protection Regulation (GDPR) 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.

A Privacy Impact Assessment was completed in February 2017 in preparation of the national clinical audits being transferred to Barts Health NHS Trust on 1 July 2017. The DPIA was updated on 06 September 2019 to include patient identifiable data flow for the national cardiac audit programme (NCAP) from Scottish hospitals. The DPIA has been reviewed and updated on 2 September 2020 to reflect the data flows from the direct contract for NCAP funding between Barts Health (NICOR) the Scottish Government from 24 June 2020.

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

The National Cardiac Audit Programme (NCAP) is managed by the National Institute for Cardiovascular Outcomes Research (NICOR) and is hosted at the Barts Heart Centre within Barts Health NHS Trust. The programme uses national clinical audit data to improve the quality of care and outcomes of patients with cardiovascular disease. The NCAP data is used for research purposes including onward sharing of data with external researchers. The NCAP programme consists of six national clinical cardiac audits which are clinically led by the relevant professional societies. The specific type of patients covered (from both the NHS and private hospitals) by each audit / specialist domain of NCAP is listed below:

1. Myocardial Ischaemia National Audit Project (MINAP) - All heart attack patients.
2. National Adult Cardiac Surgery Audit (NACSA) - All patients undergoing major heart surgery.
3. National Heart Failure Audit (NHFA) - All patients with an unscheduled admission to hospital with heart failure.
4. National Congenital Heart Disease Audit (NCHDA) - All cardiac or intrathoracic great vessel procedures carried out in patients under the age of 16 years. All adult congenital cardiac procedures performed for a cardiac defect present from birth.
5. National Audit of Cardiac Rhythm Management (NACRM) - All patients with implanted devices or receiving interventional procedures for the management of cardiac rhythm disorders.
6. National Audit for Percutaneous Coronary Intervention (NAPCI) - All patients who receive a percutaneous coronary intervention (PCI) procedure.

The population base covers patients treated in the NHS and private hospitals in England, Wales, Scotland and Northern Ireland (also includes some hospitals from the Republic of Ireland).

Purpose:

1. The delivery of Cardiovascular Quality Assessment and Quality Improvement for the NHS based upon a contract between HQIP and Barts Health (NICOR). This is currently made up of 6 NCAP domains as listed above. The Scottish Government had agreed to fund, initially via HQIP, but more recently (since 24 June 2020) as a direct contract with Barts Health NHS Trust (NICOR) for 4 of the six NCAP Specialist Domains. The intent is to increase the number of areas audited to all six domains of NCAP from April 2021.
2. NICOR also manages similar work (funded by NHS England) for the UK Transcatheter Aortic Valve Implantation (TAVI) Registry and other registries for cardiovascular new health technologies /devices.
3. Analysis of existing datasets is undertaken to provide comparative baseline data for the audit and further enrich the cardiovascular disease (CVD) audit data. Linkages to Patient Episode Database for Wales (PEDW), Hospital Episode Statistics (HES) and ONS mortality data are performed at patient level to provide information on trends in patient characteristics, treatments received and outcomes (complications, readmissions and mortality). This is expected to be replicated with the Scottish mortality and Hospital Episode Statistics data.
4. Other uses of the audit data, under contract to improve the cost-effective delivery of cardiovascular NHS care.
5. Approved research uses of the above data, including onward sharing of NCAP data for research purposes. Our CAG approval covers linkages of NCAP data from England and Wales with ONS civil registrations and HES data for audit and research purposes. Additionally, our Research Ethics Committee approval also covers us for using the linked data for research purposes including onward sharing of anonymised and linked NCAP data with civil registrations and HES data. (This will occur once a DSA with NHS Digital has been established).

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.

The DPO and the Head of Information Governance at Barts Health NHS Trust (Barts Health) have been consulted during the preparation and updating of this DPIA document (28 Sept 2020). The DPO has approved this version of the DPIA.

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.

NICOR's Patient Representatives Group (PRG). Date consulted: October 2017 and subsequent meetings of the PRG including 13 June 2019 Method of consultation: Verbal discussion between members of the Patient advisory groups. Further consultation is planned.

Internal all NICOR Staff meeting Date consulted: February 2018 Method of consultation: Verbal discussion as part of an agenda item. Further consultation is planned as part of staff training / awareness.

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.

We expect to publish the DPIA on the NICOR website: https://www.nicor.org.uk as soon as PBPP has accepted it.

Data Information Flows

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.

PERSONAL DATA COLLECTED FOR THE NATIONAL CARDIAC AUDIT PROGRAMME

The NCAP uses a sophisticated IT-based system that links data entry from NHS and private hospitals in the UK (and some from Republic of Ireland) with a secure central database. Personal data is collected and retained in a secure web based data collection interfaces which are provided to hospitals for their audit data submissions. The information recorded by hospitals include patients and the clinical care they have received.

The data can be submitted directly (direct input) or imported (indirect input) via local cardiac speciality clinical systems. Opening a database allows users to see all the records to which they have authorised access, and in turn allows the creation of new records (either by directly inputting the data or by importing data from third party systems), or editing existing information. Hospitals can export the data they have submitted using an export tool. Collected data is made secure (through encryption), anonymised (reversibly), aggregated and analysed in a single central location.

The system can be accessed via the Health and Social Care Network (HSCN) and the internet. The data is managed within a secure environment for both storage and processing. Access to servers which the data resides on is by certain staff who are responsible for manging the data. Security mechanisms are in place to not only avoid loss of data but also ensure that only authorised users access have access to information held centrally. Hospitals and individual users only see records (containing personal data) submitted by their own organisation and any published information contains only comparative analysis figures. Online reports are provided for participating hospitals that compare their performance with others and against good practice standards. Personal data is used for requests from mortuaries and funeral directors to provide implanted device information in the National Audit of Cardiac Rhythm Management.

The following Personal data is collected / used within the national clinical audit programme.

- Patient Forename (description: Records Forename)
- Patient Surname (description: Records Surname)
- Hospital Number / Local Patient Identifier (description: Hospital, serial, or another anonymous hospital generated number)
- NHS Number/CHI Number in Scotland (description: The patient's unique 10-digit NHS Number)
- Postcode of usual address at date of diagnosis (description: Patients postcode)
- Date of Birth (description: The Patient's date of Birth)
- Date of death (description: The date the patient died. Left blank if the patient is alive)

The patient forename and surname are not extracted from the database or used in any analysis. Patients can choose to opt-out of the audit, such that their details will not be stored or used for any purpose by NICOR.
The NHS Number (or the CHI Number) is not provided for analysis. The pseudonymised identifiers for the NHS number and hospital number are provided internally to the analytical team and externally to researchers instead of the NHS Number. This enables them to link data to examine for example admission patterns.

A number of data transformations are in place to reduce identifiability and sensitivity of data items. For example, postcode is converted to deprivation index; date of birth is converted to age, which is used in producing audit analysis. The NHS number is validated and retained as a unique identifier for conducting data linkage to other data sets (e.g. ONS mortality data, Hospital Episode Statistics, PEDW data).

NICOR staff who undertake analyses for publication by hospital, unit, and clinician level are not permitted to access identifiable data. The only exception to this is the analyst working with the National Congenital Heart Disease Audit data. This is so that he can identify discrepant data, e.g. incorrect weights, date of births, diagnosis and procedure information etc. which can be communicated back to hospitals for correction and resubmission.

It is important to stress that the reason why the audits collect identifiable information is so that the outcome of different treatments and care providers can be assessed. To do so the audits need to calculate how long a patient survives after treatment. A unique patient identifier must be retained so that records of treatment can be linked to subsequent date of death, even though this will often be years in the future. This allows lessons to be learnt and patient care to improve over time – the procedures that give the best survival can be promoted, and care providers who have significantly poorer safety records can be identified. Only the hospitals providing the data and staff with access to encryption keys to perform linkage with mortality data (ONS) can access patient identifiable information. All analyses and reports will not contain NHS numbers or other information that can be used to identify anyone. Throughout the entire process, strict security measures are in place to safeguard patient information

Personal data for the national clinical audit is retained indefinitely. The justification of this is that the data is required for longitudinal analyses of trends in clinical practice outcomes and Quality Improvement. The minimum retention period for all NICOR audit records is 8 years; this is consistent with NHS Retention and Disposal Schedule guidelines. There is no maximum retention period. All records identified for retention for a period greater than 8 years are subject to review and justification, including specific outcomes and level of statistical merit derived from the individual audits by audit project groups. The disposal of any data will be clearly documented including date of disposal and the type of the data destroyed. Disposal methods include secure destruction of computer media in which the backups are held and the erasure of data from NICOR servers to the current NHS guidelines / standards.

Under GDPR the legal basis for data processing by NICOR is: Articles 6(1)(E) and 9(2)(I). The Common law Duty of confidentiality is met through Section 251 Exemption of NHS Act 2006 (CAG Approval) for the NHS hospitals in England and Wales, PBPP approval in Scotland and through informed consent for the private hospitals.

RESEARCH

The NCAP data is also used for research both internally by NICOR and by onward sharing with external researchers. This is covered in England and Wales by approval from the Secretary of State for Health and Social Care under Section 251 of the NHS Act 2006 (CAG approval).

Recently NICOR provided information to the UK Government's Scientific Advisory Group for Emergencies (SAGE). This also involved COVID-19 related research conducted in collaboration with NHS Digital, Public Health England and researchers from Keele, Oxford and Leeds Universities. The NCAP and TAVI registry data for England was provided to NHS Digital for linkages with ONS civil registrations, HES data and with COVID-19 data from Public Health England for research on the impact of COVID-19 on cardiovascular disease. The legal basis for provision of this data by NICOR is covered in the Direction to NHS Digital by the Secretary of State under Section 254 of the Act to establish and operate a system for the collection and analysis of the information specified for this service for COVID-19 purposes. This also includes onward sharing of NCAP and TAVI registry data by NHS Digital with third party researchers for COVID-19 related research.

OTHER PERSONAL DATA COLLECTED

We also collect personal data and contact details, on informed consent basis, of the clinical audit leads and the audit team members at the hospitals participating in NCAP. This data is not part of the NCAP dataset, but it is used to communicate with and support the hospital audit teams that submit NCAP data to NICOR. We also collect similar personal data and contact details, on informed consent basis, of other NCAP stakeholder groups (e.g. patient representative group that we need to consult, as well as). It is primarily used for communicating with the clinical audit teams at the hospitals (national clinical audit/research related news emails and newsletters) and hospital registrations to the audit programme. The information is kept on a central file share per audit/domain and is managed by the project management team. Individuals can request for their information to be changed / deleted. The types of personal data collected for this purpose includes the individual full name, email, and telephone number.

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).

No personal date will 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	Yes		To assist linkage at ONS/ NHS Digital data linkages service.
NHS number	Yes		Used for unique identification to match records from different service providers. To assist linkage at ONS/ NHS Digital data linkages service.
Address		N/A	
Postcode	Yes		In some audits, the address at diagnosis is used to enable analysis by locality of patients, report on inequalities in access to care and in case mix adjustment. Post code is converted to CCG code, LAT / NHS team code, and deprivation score and easting and northings (rounded to 1km).

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]*
Date of birth	Yes		To enable age at diagnosis to be established for epidemiological and survival analyses. To enable analysis by birth cohort and to assist linkage at NHS Digital (and registries) for women who have changed their name on marriage (or back on separation/divorce).
Date of death	Yes		To determine post-operative survival rates and mortality rates
Age		N/A	
Sex	Yes		Used for audit analysis purposes
Marital Status	No	N/A	
Gender	Yes		Used for audit analysis purposes
Living Habits	No	N/A	
Professional Training / Awards	No	N/A	
Income / Financial / Tax Situation	No	N/A	
Email Address	No	N/A	The only emails that we collect are those of the clinical audit team members (not patients) supplying the audit data to NICOR. This is used for communication purposes only.
Physical Description	No	N/A	
General Identifier e.g. Hospital No	Yes		To enable the generation of a unique ID for each patient. Important where hospitals are unable to provide a valid NHS number. Used to validate NHS number being used is correct
Home Phone Number	No	N/A	
Online Identifier e.g. IP Address/Event Logs	No	N/A	
Website Cookies	No	N/A	
Mobile Phone / Device No	No	N/A	The only phone numbers that we collect are those of the clinical team members (not patients) supplying the audit data for communication purposes only.
Device Mobile Phone / Device IMEI No	No	N/A	
Location Data (Travel / GPS / GSM Data)	No	N/A	
Device MAC Address (Wireless Network Interface)	No	N/A	
Sensitive Personal Data			
Physical / Mental Health or Condition	Yes		Variable such as the condition being treated, diagnosis, procedure being performed etc is collected and used for analysis/reporting purposes.

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]*
Sexual Life / Orientation		N/A	
Family / Lifestyle / Social Circumstance		N/A	
Offences Committed / Alleged to have Committed		N/A	
Criminal Proceedings / Outcomes / Sentence		N/A	
Education / Professional Training		N/A	
Employment / Career History		N/A	
Financial Affairs		N/A	
Religion or Other Beliefs		N/A	
Trade Union membership		N/A	
Racial / Ethnic Origin	Yes		Used for analysis purposes
Biometric Data (Fingerprints / Facial Recognition)		N/A	
Genetic Data		N/A	
Spare			

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.

Hospitals / providers who participate in the audit programme are responsible for ensuring the personal data they submit is accurate and up to date.

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.

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 Privacy notice	This is detailed in our Privacy-Fair Processing leaflet dated 21-10-2020, see attached, published on NICOR website.	Any patient wishing to OPT OUT of data sharing/linkage can do so by writing to James Chal, NICOR Chief Operating Officer, at the address below or by leaving contact details on the telephone number or email below and this will not affect the quality of their healthcare. You also have the right to request a copy of any information NICOR hold on you and to request rectification of this information. You can do this by making a Subject Access Request to James Chal at the below address. If you are not satisfied with NICOR's response you have the right to make a complaint to the Information Commissioner's Office (ICO) https://ico.org.uk/
Individuals can access information held about them	Included in Privacy notice	This is detailed in our Privacy-Fair Processing leaflet dated 21-10-2020, see attached, published on NICOR website.	You can do this by writing to your consultant at the hospital that provides your care or to James Chal at NICOR using the email address/postal address below. Your consultant or NICOR would be able to provide you a copy of your information that is held at NICOR. It would be sent to you either as a paper record or as encrypted data on a CD/Pen drive, which would be sent to you by recorded delivery. Alternatively we can make your data available to you electronically via the NICOR's secure Dropbox. In order to access your data electronically we require your personal email address and a contact phone number. Once we have uploaded your data file we

			would need to contact you to give you the password to access your encrypted file.
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 Privacy notice	This is detailed in our Privacy-Fair Processing leaflet dated 21-10-2020, see attached, published on NICOR website.	Due to the nature of national clinical audit for which we need to include as many patients as possible, we are not able to erase your data. However, you do have the option to opt-out, as described above.
Rectification of inaccurate information	Included in Privacy notice	This is detailed in our Privacy-Fair Processing leaflet dated 21-10-2020, see attached, published on NICOR website.	You can also request rectification of any inaccuracies of your information. You can do this by writing to your consultant at the hospital that provides your care or by making to a Subject Access Request to James Chal at the address below.
Restriction of some processing	N/A	Unless patients have opted out we process all data submitted.	
Object to processing undertaken on some legal bases	Included in the Privacy Notice	Unless patients have opted out we process all data submitted.	Whilst the National Data Opt-out Policy only applies in England, patients in other parts of UK can still object to the use of their data for this audit by their doctor responsible for their care or to NICOR as detailed below.
Complain to the Information Commissioner's Office;	Included in Privacy notice	This is detailed in our Privacy-Fair Processing leaflet dated 21-10-2020, see attached, published on NICOR website.	If you are not satisfied with NICOR's response you have the right to make a complaint to the Information Commissioner's Office (ICO) https://ico.org.uk/
Withdraw consent at any time (if processing is based on consent)	N/A		
Data portability (if relevant)	N/A		
Individual knows the identity and contact details of the data controller and the data controllers data protection officer	Data controllers are detailed in the NICOR – Privacy and Fair Processing Patient and Public Information.	This is detailed in our Privacy-Fair Processing leaflet dated 21-10-2020, see attached, published on NICOR website.	
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	This is detailed in our Privacy-Fair Processing leaflet dated 05-10-2020, see attached, published on NICOR website.	NICOR only processes data in England. If we need to transfer any data outside of the UK for any purposes we will ensure that we have appropriate permissions/approvals in place before the transfer can take place.	Although we receive patient data from the United Kingdom and Ireland NICOR only process the data in England. If any data is required to be transferred outside of the UK for any purposes (audit or research) we will ensure that we have all appropriate

recipient is in an 'adequate' country / how a copy of the safeguards can be obtained.			permissions/approvals in place before the transfer can take place.
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 Privacy notice	This is detailed in our Privacy-Fair Processing leaflet dated 21-10-2020, see attached, published on NICOR website.	In accordance with these regulations and approval from the Secretary of State for Health and Social Care, the NCAP is permitted to collect, use and store patient data from England, Wales and Scotland without consent. However, the legal basis for collecting and processing NCAP data from the private healthcare providers is informed consent. NICOR is the legal data processor of the NCAP data for which HQIP is the data controller. The legal basis for data collection and processing is given at the bottom of this document*. Under GDPR it is Article 6(1)(e) and Article 9(2)(i) and the common law duty of confidentiality is met by section 251 exemption or informed consent.
To know the purpose(s) for the processing of their information.	Included in Privacy notice	This is detailed in our Privacy-Fair Processing leaflet dated 21-10-2020, see attached, published on NICOR website.	The information collected is used to check that hospitals providing care are following national guidance. NICOR produces annual reports which assess the care and treatment of all patients in the UK and Ireland. We produce reports every year to assess performance against national standards and review improvements that have been made. The reports are available to the Department of Health, the Welsh and Scottish Governments, patients and the public, participating hospitals, healthcare commissioners, clinicians, Care Quality Commission and hospital management. The reports are available on the NICOR web pages https://www.nicor.org.uk/national-cardiac-audit-programme/
Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the	N/A		

personal data.			
The source of the data (where the data were not collected from the data subject)	Included in Privacy notice	This is detailed in our Privacy-Fair Processing leaflet dated 21-10-2020, see attached, published on NICOR website.	Barts Health NHS Trust (Barts Health) hosts **the National Cardiac Audit Programme (NCAP)** which collects Relevant Personal Data (including personal health and demographic details) and reports on patient data from all NHS and private hospitals from throughout the UK and Ireland
Categories of data being processed	Included in Privacy notice	This is detailed in our Privacy-Fair Processing leaflet dated 21-10-2020, see attached, published on NICOR website.	Barts Health NHS Trust (Barts Health) hosts **the National Cardiac Audit Programme (NCAP)** which collects Relevant Personal Data (including personal health and demographic details) and reports on patient data from all NHS and private hospitals from throughout the UK and Ireland
Recipients or categories of recipients	Only anonymised information is shared with recipients (unless they have appropriate approvals)	This is detailed in our Privacy-Fair Processing leaflet dated 21-10-2020, see attached, published on NICOR website.	Analyses, reports and data derived from our audits and registries, which may be used for research purposes, are anonymised and do not contain any information that can be used to identify individual patients (unless appropriate approvals have been granted to the researchers by the Secretary of State for Health and Social Care, the Research Ethics Committee and the appropriate data controllers).
The source of the personal data	Included in Privacy notice	This is detailed in our Privacy-Fair Processing leaflet dated 21-10-2020, see attached, published on NICOR website.	Hospitals from Northern Ireland, UK independent healthcare sector and the Republic of Ireland (RoI) submit data for NCAP purposes.
To know the period for which their data will be stored (or the criteria used to determine that period)	Included in Privacy notice	This is detailed in our Privacy-Fair Processing leaflet dated 21-10-2020, see attached, published on NICOR website.	An audit is most effective when it contains information from every patient. Patient details help teams to learn how best to treat heart disease, make sure they provide the best care and help find out the causes of heart disease. Personal data for the national clinical audits and registries is retained indefinitely. The reason for this is that long-term longitudinal data (over many years) is required for trend analyses to demonstrate variations and changes in clinical practice and for improvements in quality of care. The minimum retention period for all NICOR audit records is 8 years; this is

			consistent with NHS Retention and Disposal Schedule guidelines.
The existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects (if applicable)	N/A		

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.

Total number of unique records - 4,734,100 Annual growth across all six domains - 313,000

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

Please see appendix 2 for additional guidance on completing this table

What are the potential risks to the individuals whose personal data you hold?	**Likelihood of this happening** 1 Very unlikely 2 Unlikely 3 Possible 4 Likely 5 Very Likely (See guidance below for definition))	**Impact** 1 -Insignificant 2-Minor 3-Moderate 4-Major 5-Catastrophic (See guidance below for definition)	**Overall risk score** (likelihood x impact = score)	**Will risk be accepted, reduced or eliminated?**	**Mitigating action to reduce or eliminate each risk OR Where risk is accepted give justification.**	**Explain how this action eliminates or reduces the risk**	**Expected completion date**	**Responsible owner**
Illegitimate access, undesired modification and disappearance of data	1	5	5	**Significantly reduced**	• Recently developed modern ICT platform for data collection with strict security measures in place to safeguard any illegitimate access. There were verified by a security penetration testing completed earlier this year. • Only limited number of staff (who genuinely require it) have access to the personal data. • At the centres the staff who access the ICT platform for data entry can only see the data of their own patients. • Any modifications made are recorded in an audit	These security measures reduce this risk significantly.		James Chal

					log (who made what changes). • There is a back up of the database made every day. If any data disappears for any reason it can be repopulated from the back up.			
Disclosure of personal / confidential information thus potential breach to DPA and other standards / legislation and local policies	1	5	5	**Eliminated**	• Personal data is encrypted and held on secure servers at a secure external data centre • Access to the data is via secure logins • Staff who are responsible for managing the data / preparing data for linkage / extraction purposes only have access • SOP's, procedure and guidelines • Information governance awareness / training for all staff	Confidentiality mechanisms as described have been designed to ensure that only authorised people can access the information on the database - users can only see records submitted by their own organisation		James Chal
Interception of personal /confidential information by third party during transfer	1	5	5	**Eliminated**	• Data is transferred using secure encrypted file transfer facilities. • Data transmission process are encrypted • Access is managed through appropriate	The security of the data is maintained at all times using these control measures		James Chal

					rights controls			
Transfer of personal / confidential information to researchers	1	5	5	**Eliminated**	• Deidentified data is sent, e.g. instead of DOB calculated age is provided; operator details are pseudonymised; no patients details are provided; NHS number is pseudonymised. Post code is converted to CCG code, LAT / NHS team code, and deprivation score and easting and northings (rounded to 1km). • Pre-release process ensure appropriateness by screening data extracts for confidential information before onward transfer	Only anonymised data is provided to researchers. No personal data is release except in instances where the appropriate permissions / approval are in place (e.g. section 251)		James Chal
Corporate risks & compliance risks section								

Regularly reviewing the DPIA

DPIA should be an ongoing process and regularly reviewed during the lifecycle of the project or programme to ensure

- Risks identified are still relevant
- Actions recommended to mitigate the risks have been implemented and mitigating actions are successful

You must add to your DPIA every time you make changes to the existing projects, send an updated version to your HQIP project manager and ensure that you incorporate any identified risks/issues to your risk/issue registers of the project contract review form.

Appendix 1 Submitting your own version of DPIA

If submitting your own version of DPIA please ensure it includes the following items. If any items are missing please add this to your DPIA and then submit it. You must also complete the screening questions above.

	Checkbox – Please tick	Evidence – Page number and section in your DPIA
Confirmation of advice /consultation sought from Data Protection Officer whilst completing the DPIA	**YES**	**Page 8 (DPIA consultation)**
Name of DPO (Interim)	**YES**	**Sarah Palmer-Edwards**
Name and role of person approving completion of DPIA form. This must not be the same person that completes the form.	**YES**	**Sarah Palmer-Edwards, Head of Information Governance/DPO, Barts Health NHS Trust**
Will the DPIA be published or part of it such as the summary or conclusion (not essential but encouraged). If so, where is it published?	**YES**	**NICOR website: https://www.nicor.org.uk**
Does it include a systematic description of the proposed processing operation and its purpose?	**YES**	
Does it include the nature, scope, context and purposes of the processing	**YES**	
Does it include personal data, recipients and period for which the personal data will be stored are recorded	**YES**	
Does it include the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels)	**YES**	
Does the DPIA explain how each individual's rights are Managed? See section on individuals rights	**YES**	
Are safeguards in place surrounding international transfer? See section on sending information outside the EEA	**N/A**	**Data is processed in England only. However, should the need arise, all necessary permissions will be secured prior to any international data transfer.**
Was consultation of the document carried out and with whom?	**YES**	**Detailed in the DPIA with Patient Representative Group and NICOR staff**
Organisations ICO registration number	**YES**	Z3086438
Organisations ICO registration expiry date	**YES**	29 March 2021
Version number of the DPIA you are submitting	**YES**	**Version 2.0 (21 October 2020)**
Date completed	**YES**	**21 October 2020**

Appendix 2 Guidance for completing the table

<table>
<tr><td>What are the potential risks to the individuals whose personal data you hold?</td><td>See examples above</td></tr>
<tr><td>Likelihood of this happening (H,M,L)</td><td>
<table>
<tr><th>Likelihood score</th><th>Description</th><th>Example</th></tr>
<tr><td>1</td><td>Very unlikely</td><td>May only occur in exceptional circumstances</td></tr>
<tr><td>2</td><td>Unlikely</td><td>Could occur at some time but unlikely</td></tr>
<tr><td>3</td><td>Possible</td><td>May occur at some time</td></tr>
<tr><td>4</td><td>Likely</td><td>Will probably occur / re-occur at some point</td></tr>
<tr><td>5</td><td>Very likely</td><td>Almost certain to occur / re-occur</td></tr>
</table>
</td></tr>
<tr><td>Impact (H,M,L)</td><td>
<table>
<tr><th>Impact scores</th><th>Description</th><th>Example</th></tr>
<tr><td>1</td><td>Insignificant</td><td>No financial loss; disruption to day to day work manageable within existing systems, no personal data loss/ no breach of confidentiality</td></tr>
<tr><td>2</td><td>Minor</td><td>Minor (<£100k) financial loss / disruption to systems; procedures require review but manageable; limited slippage in work activity, breach of confidentiality where < 20 records affected or risk assessed as low where data pseudonymised/files encrypted and no sensitive data</td></tr>
<tr><td>3</td><td>Moderate</td><td>Disruption to financial systems (<£250k); significant slippage in work activity or resources e.g. delay in recruiting staff; procedures and protocols require significant review, breach of confidentiality/ loss personal data where < 100 records involved and no sensitive data</td></tr>
</table>
</td></tr>
</table>

	4	Major	Major financial loss (£500k); large scale disruption to deliverables & project plans; business activity severely undermined, wasting considerable time / resources; poor quality report leading to loss of confidence in provider / HQIP / NHSE, breach of confidentiality/loss of personal sensitive data or up to 1000 records
	5	Catastrophic	Huge financial loss (>£500k); significant threat to viability of the organisation in total or in part; huge disruption to business activity; almost total lack of confidence in project provider / HQIP / NHSE, serious breach of confidentiality/loss of personal sensitive data >1000 records involved

Risk score (calculated field)	Please multiply the likelihood by the severity (likelihood x severity = risk score). This score will help to rank the risk so the most severe risks are addressed first
Will risk be accepted, reduced or eliminated? (where risk is accepted give justification)	A = Accepted (must give rationale/justification) R = Reduced E = Eliminated
Mitigating action to reduce or eliminate each risk	Insert here any proposed solutions – see managing privacy and related risks section above OR If a risk has been accepted please give justification here (The purpose of the DPIA is to reduce the risk impact to an acceptable level while still allowing a useful project to be implemented.)
Explain how this action eliminates or reduces the risk	Describe how your proposed action eliminates or reduces the possible risk. You may want to assess the costs/resource requirements (i.e. purchasing additional software to give greater control over data access and retention) and balance these against the benefits, for example the increased assurance against a data breach, and the reduced risk of regulatory action and reputational damage.
Expected completion date	What is the expected completion date for your proposed action? Ensure that DPIA actions are integrated into the project plan. You should continue to use the PIA throughout the project lifecycle when appropriate. The DPIA should be referred to if the project is reviewed or expanded in the future.
Action Owner	Who is responsible for this action?