Data Protection Impact Assessment for National Respiratory Audit Programme (NRAP)

Document control:

	Name and role	Contact details
Document Completed by	Peter Van Geffen, NRAP Project Manager	peter.van-geffen@rcp.ac.uk
Data Protection Officer name	Pamela Forde	pamela.forde@rcp.ac.uk
Document approved by (this should not be the same person that completes the form).	Lara Amusan Programme Manager	lara.amusan@rcp.ac.uk
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	Z7085833 (Expiry: 16 September 2025)	

Date Completed	Version	Summary of changes
12 April 2018	V1.0	HQIP template
30 April 2018	V4.0	Initial drafts and changes made as result of consultation
25 July 2018	V5.0	Changes made as requested by Public Benefit and Privacy Panel, Scotland
31 July 2018	V5.2	Further changes made as requested by Public Benefit and Privacy Panel, Scotland
03 August 2018	V5.3	Further changes made as requested by Public Benefit and Privacy Panel, Scotland
06 August 2018	V5.4	Further changes made as requested by Public Benefit and Privacy Panel, Scotland
4 February 2019	V5.5	DPIA reviewed and updated (routine 6-monthly process)
18 October 2019	V5.6	DPIA reviewed and updated (routine review)
19 February 2020	V5.7	DPIA reviewed and updated
01 June 2020	V8.1	DPIA reviewed and updated in light of changes to data flows and IG amendments made in May – June 2020
19 April 2021	V8.2	DPIA reviewed and updated in April 2021
20 October 2021	V8.3	DPIA reviewed and updated in October 2021
18 January 2022	V8.4	DPIA reviewed and updated in January 2022
15 June 2022	V8.5	DPIA reviewed and updated in June 2022
14 October 2022	V8.6	DPIA reviewed and updated in October 2022
01 December 2023	V9.0	DPIA reviewed and updated November 2023 to include audit name change as of 01 June 2023, updated CAG information.
26 March 2024	V10.0	DPIA reviewed and updated to include change to pulmonary rehabilitation CAG information.
16 December 2024	V10.1	DPIA reviewed and updated to include HQIP overarching research CAG (24/CAG/0108)
31 March 2025	V10.2	DPIA reviewed and updated in March 2025.

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?	No		
2	Does your project involve any sensitive information or information of a highly personal nature?	Yes		Secondary care components (adult asthma, children and young people asthma and Chronic Obstructive Pulmonary Disease (COPD)) include the collection of patient identifiable information: • NHS number • Date of birth / date of death • Postcode Approval to collect this information in **England and Wales** is gained via section 251 application and approval process. • adult asthma and COPD audits: 23/CAG/0045; • children and young people asthma audit: 19/CAG/0001); • pulmonary rehabilitation audit: 23/CAG/0167. In addition to this, local Caldicott Guardian approval is obtained for each participating hospital. All secondary care audits require identifiable hospital staff user information (name, email address, telephone number, place of work). Users voluntarily register themselves on the NRAP web-tool to participate in the audits. In addition to this, local Caldicott Guardian approval is obtained for each participating hospital.
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?	Yes		The audit programme will involve collection of data for: **Children:** the children and young people asthma audit collects data pertaining to children and young people, aged 1-18 inclusive, who are admitted to hospital for an asthma attack. Data will only be collected to assess the

	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.			extent to which the care received meets guidelines and standards to enable services to improve care. **Elderly:** the adult asthma, COPD and PR audits collect data pertaining to elderly people (they do not have an upper age limit), who are admitted to hospital with an exacerbation of asthma or COPD or enrolled onto pulmonary rehabilitation. Data will only be collected to assess the extent to which the care received meets guidelines and standards to enable services to improve care.
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?	No		
5.	Does your project match data or combine datasets from different sources?	Yes		**England and Wales** Patient identifiers are used to link with: • England - Hospital Episode Statistics (HES) Admitted Patient Care (APC) dataset for patient admission and readmission data • Wales – Patient Episode Database of Wales (PEDW) via Digital Health and Care Wales (DHCW) for admission and readmission data • England and Wales - Office for National Statistics (ONS) via NHS England for patient mortality data
6.	Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	No		Information is gathered from hospitals, GP practices and PR services. • Posters and patient information flyers are provided and detail how and why data is used and what security measures are taken to ensure its security. • Fair processing notices are also available for each workstream and an NRAP wide privacy notice is available via https://www.rcplondon.ac.uk/projects/information-governance .
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 Respiratory Audit Programme (NRAP) is the new name for the audit and will continue to run as per previous versions of the audit until at least 31 May 2026 - following the commencement of the new contract in June 2023. *Previous contract name 'National Asthma and COPD Audit Programme' (NACAP)* **Hospital and service user details** The audits delivered by NRAP (COPD, adult asthma, children and young people asthma and PR) continue to require hospital and PR service user information as data must be entered and signed off by clinical staff. Users voluntarily register themselves on the NRAP web-tool to participate in the audits. **Pulmonary Rehabilitation audit expansion** ○ As of 01 November 2023, the PR audit has expanded to include patients who are referred for pulmonary rehabilitation with the following patient primary disease - COPD, asthma, bronchiectasis, interstitial lung disease, long covid, other chronic respiratory disease, pre/post thoracic surgery (including lung cancer/LVR/lung transplant), pulmonary hypertension, chronic heart failure.

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 started on 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 if 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.

This DPIA was originally completed in April 2018 and has been updated several times since (current version 10.0). The original draft was completed both in retrospect (in terms of the secondary care COPD continuous clinical audit component of NACAP, which started in February 2017) and at the planning stage (in terms of the asthma and PR audits). The adult asthma audit launched in November 2018 and PR and children and young people asthma audits launched in March and June 2019 respectively. NACAP became NRAP on the 01 June 2023 and will continue working in accordance with this data protection impact assessment.

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

Aim

The overall aim of NRAP is to improve the care, experiences and outcomes of patients with respiratory disease (including asthma and COPD). It provides healthcare services with the information and tools they need for healthcare improvement (HI) and service development to ensure that patient care and experience is of the highest possible standard.

The Royal College of Physicians (NRAP) will aim to capture <u>all eligible patients:</u>

1. Admitted to hospitals (in England and Wales):

1.1 The children and young people asthma audit will collect data on patients:

- who are between 1 and 5 years old on the date of arrival and have been admitted to a hospital paediatric service with a primary diagnosis of an asthma attack OR a primary diagnosis of wheeze AND a secondary diagnosis of asthma (include patients where this was initially unclear, but later identified as an asthma attack/wheeze AND asthma attack)
- who are between 6 and 18 years old on the date of arrival and have been admitted to a hospital paediatric service with a primary diagnosis of an asthma attack.

1.2 The adult asthma audit will collect data on patients:

- who are 16 years and over on the date of arrival,
- who have been admitted to hospital adult services,
- who have a primary diagnosis of asthma attack,
- where an initial, or unclear, diagnosis is revised to asthma attack.

1.3 The COPD audit will collect data on patients:

- who are 35 years and over on the date of admission,
- who have been admitted to hospital adult services,
- who have a primary diagnosis of COPD exacerbation,
- where an initial, or unclear, diagnosis is revised to an acute exacerbation of chronic obstructive pulmonary disease (AECOPD).

2 Pulmonary Rehabilitation in England and Wales

2.1 The PR audit will collect data on patients:

- who attend an initial assessment for pulmonary rehabilitation
- who have a primary diagnosis of COPD, asthma, bronchiectasis, interstitial lung disease, long covid, other chronic respiratory disease, pre/post thoracic surgery (including lung cancer/LVR/lung transplant), pulmonary hypertension, chronic heart failure or other chronic respiratory disease
- who are 18 years or over on the date of assessment.

3 Primary Care Wales audit

3.1 The primary care Wales audit conditions for data collection*:

- The patient is registered with a practice in Wales on the first day of the extraction period,
- The patient is deemed to have COPD or asthma based on the presence of a validated Read code,
- The full list of Read codes used for the primary care audit will be available before the extraction takes place on the NRAP resources webpage (https://www.rcplondon.ac.uk/projects/outputs/support-service-teams-primary-care),
- The patient is aged 18 or over on the first day of the extraction period if they are recorded as having COPD.
- The patient is aged 1 or over (to distinguish between wheezy infants that are not asthmatics and those where an official diagnosis has been made) on the first day of the extraction period.

* This audit does not require Confidentiality Advisory Group (CAG) approval as no patient identifiable information is collected. It is not subject to Common Law Duty of Confidentiality and patient consent is not required. The audit is supported by Welsh Government and is approved by the Data Quality System Governance Group.

between the launch of the audits (which were staggered) and the programme end (currently May 2026).

Data processing

Secondary care and pulmonary rehabilitation (PR) components

Data is currently collected for all admissions to hospital for acute exacerbation of COPD, adults with asthma and children and young people with asthma in England and Wales, on a continuous basis from those hospitals who have registered to take part in NRAP.

The PR audit launched in March 2019; and continuously collected information on patients with COPD referred to and assessed for PR in England and Wales. As of the 01 November 2023 the PR dataset was expanded to include, not only COPD patients referred to PR, but also to include patients where their primary disease is one of the following: COPD, asthma, bronchiectasis, interstitial lung disease, long covid, other chronic respiratory disease, pre/post thoracic surgery (including lung cancer/LVR/lung transplant), pulmonary hypertension, chronic heart failure.

Local sites enter audit data for appropriate patients via a bespoke web-tool hosted by Crown Informatics (www.nrap.org.uk). Raw, unadjusted data at site-level (non patient-identifiable) are presented on run charts and benchmarking tables in near to real time (one month after data submission). The run charts became publicly available on the 01 August 2022, supporting local HI. The benchmarking tables were released into the public domain during December 2023.

Patient identifiable data is only visible to registered users of the individual hospital site / service, and to Crown Informatics (webtool host), if required for administrative purposes. Please note, Crown only access the data on very rare occasions, examples of which are listed below:

- System 'de-bugging' investigations if problems are experienced with processes where patient identifiable data is involved. Examples might include duplicate checks, re-admission processing, and validation processing. Note, wherever possible, system tests are undertaken on test systems using dummy/fake patient identifiable data. However, processing of live data may have to be examined in detail in rare but limited circumstances.
- Data linkage exercises to validate linkage success - this is usually limited to spot checks. Bulk access to patient identifiable data is necessary to undertake linkage exercises (i.e. to prepare the files for transfer to NHS England or DHCW).
- Subject access requests - when a patient requests their audit details.

No other organisation or individual will be able to access these identifiable data.

Once a year, Crown Informatics will extract patient-level data from the web-tool for the purpose of the annual national report. Reporting cohorts are determined by the date of the patient's discharge (in secondary care) or of assessment/commencement of a programme (in PR). For example, a report will contain the cohort discharged from hospital/who commenced PR between 1 April 2024 and 31 March 2025 in England and Wales. Sites will have 6 weeks from the end of the patient cohort period to enter the data prior to it being extracted by Crown. For PR services this is 18 weeks to ensure patients have enough time to complete their PR programme. This is communicated to services on the log-in page of the web-tool, but also via email and other methods of communication. This delay ensures that the hospitals/services have had the time to a) if necessary, retrieve notes, and b) manually enter the data into the system.

Once extracted, Crown will anonymise these data using the following methods:

- NHS number will be replaced by study ID
- Postcode will be reduced to the first 4 digits (also known as 'Lower Super Output Area (LSOA)', needed for derivation of deprivation indices)
- Date of birth will be transformed to month and year of birth.

Once the data have been anonymised, Crown will transfer patient-level (anonymised) data for the full report cohort (England and Wales) to Imperial College London (ICL) for data cleaning and analysis. Crown operate an 'encrypted/electronic only' data transfer policy for all patient level data using HTTPS 'web file transfer' protocols (256 Bit SSL) and store data on secure end points. Data is protected in AES-256 bit encrypted ZIP files and stored in password protected file transfer databases, which operate under secure access protocols, access logging/tracking and authentication mechanisms. Decryption password dissemination/management operates under a defined identity policy and is given or received orally by a suitably trained and IG trained senior operatives. Use of portable storage media and email is prohibited. Data processing assets are operated in secure locations.

Following the cleaning and analysis of data, aggregated (i.e. analysed and non-identifiable) data will be transferred from ICL to the RCP to provide commentary for, and then publish, audit programme outputs (e.g. national reports, site level reports) all of which will allow hospitals to gain an understanding of the extent to which the care they deliver is similar to that delivered by their peers.

In addition, in line with reporting deliverables (outcomes report), Crown Informatics will securely transfer identifiable data (NHS number, DOB and postcode) to NHS England and DHCW in order to link to HES, ONS and PEDW datasets. This will allow understanding of the longer-term outcomes for the audit cohort, namely admission/readmission and mortality rates at 1 and 3 months (secondary care). The cohort transferred to these organisations will be the same as that extracted for the purpose of the annual national report (i.e. so that a later report detailing their medium-to-long term outcomes can be published). NHS England and DHCW will return patient level pseudonymised linked data (with identifiers removed, but the unique audit identifier retained) to ICL in its role as the organisation responsible for analysis of the data. Imperial will combine the validated identifiers, outcomes data and the relevant audit data.

Following the cleaning and analysis of data, aggregated (i.e. analysed and non-identifiable) data will also be transferred from ICL to the RCP to provide commentary for, and then publish, outcome-related audit programme outputs (e.g. national reports, health board reports).

Primary care component

Primary care data are extracted from GP practices in Wales. Data is anonymised at source (no identifiable data leaves the GP practice). An Audit+[1] NRAP module will be deployed to all general practices to support QI activity and direct patient care in Wales. Aggregate general practice data will be submitted to DHCW to be processed and presented within the Primary Care Information Portal[2]. The data received will subsequently be aggregated to the Cluster, LHB and all-Wales level to enable appropriate views of the data for a "standard" user of the Primary Care Information Portal. Practices will be able to view their own data and compare it against Cluster, LHB and all-Wales figures. The NRAP and Imperial College London teams will receive anonymised, aggregated, and analysed data from DHCW in order to draft and publish appropriate outputs at two time points between 2023-2026. Previous reports can be found at www.rcp.ac.uk/pc2021.

[1] Audit+ is a software application freely available to every GP practice in Wales. Audit+ is developed and owned by Informatica Systems Ltd. and is made available to NHS Wales through the DQS contract, where DHCW has procured Audit+ on behalf of Welsh GP practices. Audit+ sits within the GP practice and extracts data from the practice's clinical system. It then analyses that data based on sets of queries deployed to Audit+ by DHCW, and then presents the results of that analysis to the GP practice in the form of patient identifiable reports, patient lists, and dashboards.

[2] The Primary Care Information Portal has been developed by and is owned by DHCW. It was originally established to serve as the platform to present the aggregate data submissions received from Audit+ to NHS Wales users, as well as provide tools and reports to support GMS Contract yearend activity. Since its inception the Portal has evolved to incorporate data and reports beyond core DQS related data (NACAP has previously utilised the Portal to present its annual report data back to NHS Wales practices and organisations).

Third party applications for data

After patient identifiers have been removed from the data in this programme, data may be used for secondary research purposes. HQIP's Overarching Research Database Approval for the NCAPOP permits this re-use under S.251 of the NHS Act 2006 (Reference 24/CAG/0108). If applying for identifiable data, a separate CAG will be required to be applied for by the researcher. The main use of data will always be to improve care and services for people with COPD. NRAP will not share any of this data unless the appropriate legal, ethical and security arrangements are in place to keep it safe and secure.

Retention of data

All data will be destroyed in line with the Information Governance Alliance (IGA)'s Records Management Code of Practice for Health and Social Care 2016 (available at: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care), which specifies that clinical audit records must be kept securely for a minimum period of 5 years after the audit has been completed. This will potentially allow post-audit queries to be answered, outstanding longitudinal analyses to be completed and for third party data requests to be approved and completed. Once the point of the audit closure has been reached, any need for retention of patient identifiable data during this period will be assessed by the funders (NHS England and Welsh Government) and the outcome of this assessment will be informed to CAG and subject to extension/amendment requests as required. The NRAP contract date currently runs until at least 31 May 2026.

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.

Project management team, Data Protection Officer, Senior Management, IT (webtool) provider, Imperial College London, Crown Informatics

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.

Version 10.2 will be published in March 2025: National Respiratory Audit Programme (NRAP) | RCP

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.

The NRAP has data flow charts for all its audit components. These can be found below.

Primary care (asthma and COPD) – Legal basis = anonymised at source

PC_Data Flow_v0.3_Septembe

Next data extraction (February 2024 – 1st August 2021-31st July 2023)

1. An Audit+ NRAP module will be deployed to all general practices to support QI activity and direct patient care in Wales. As a by-product of this module is in situ aggregate general practice data, based on the Read/SNOMED coded searches (of the live registered general practice list) contained within the module, will be submitted to DHCW to be processed and presented within the Primary Care Information Portal.
2. The data received will subsequently be aggregated to the Cluster, LHB and all-Wales level to enable appropriate views of the data for a "standard" user of the Primary Care Information Portal. Practices will be able to view their own data and compare it against Cluster, LHB and all-Wales figures.
3. As the data exported from each general practice is at the aggregate level it will not be possible to be re-identified by any party
4. DHCW will use the aggregated data to update the DHCW Primary Care Information Portal on a quarterly basis to facilitate reporting of audit results back to individual practices and produce national audit results (all Wales, cluster and LHB) at agreed points. All data will be stored on the secure DHCW server. General practices as data controllers, through functionality within the Primary Care Information Portal, have the ability to share their aggregate results with other users of the Portal. The published national reports in September 2024 and the summer of 2026 will additionally be made available to complement the quarterly reporting process.
5. The NRAP and Imperial College London teams will receive anonymised, aggregated and analysed data from DHCW in order to draft and publish appropriate outputs (national report, LHB reports, etc.). The provision of national data will be in February 2024 and August 2025. Aggregated practice level data will also be used for the purpose of audit, service evaluation and research (with appropriate ethical approvals) by approved third parties and Data Quality System (DQS) governance group if appropriate. This will involve the DHCW securely transferring anonymised, aggregated practice level data to credible applicants (i.e. those whose request has been approved by both HQIP and the NRAP).

Continued from above

Secondary care – COPD and adult asthma – 23/CAG/0045

Legal basis:

- 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.
- Article 9 (2) (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.
- 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.


AA_Data Flow_v2.0 December 2024.pdf


COPD_Data Flow_v2 December 2

Stage 1 (data entry and pseudonymisation): Local sites (i.e. clinicians, members of the audit team) enter audit data (including patient identifiable data (PID)) for appropriate patients via a bespoke web-tool hosted by Crown Informatics (www.nrap.org.uk). From 31st July 2022, local sites must also ensure that people with asthma and/or COPD within England who have set a national data opt out preference from the AA/COPD audit are not included in the data submitted to NRAP.

Crown anonymises data (audit and linked). NHS number is pseudonymised into audit ID, date of birth transformed to age, date of death is transformed into survival at x days and postcode is reduced to the first 4 digits (LSOA).

Stage 2 (audit data analysis and management): Pseudonymised patient level data is sent to ICL for data cleaning and analysis.

Stage 3 (report writing): Aggregated data is sent to RCP to draft audit outputs (e.g. national reports).

Stage 4 (linkage): Crown sends identifiable data to NHS England and DHCW for linkage purposes and asthma/COPD data is combined with HES, PEDW and ONS and then pseudonymised by NHS England and DHCW. All patient level pseudonymised linked data is returned to ICL. ICL will combine the validated identifiers, NHS England and DHCW data and the relevant audit data and carry out data cleaning and analysis activities.

Stage 5 (linked data analysis and management): Following the cleaning and analysis of data by ICL, aggregated (i.e. analysed and non-identifiable) data will also be transferred from ICL to the RCP to provide commentary for, and then publish, outcome-related audit programme outputs (e.g. national reports, all data files etc).

Stage 6 (outcome report writing): Aggregated data is sent to RCP to draft audit outputs (e.g. national reports).

Hospital level real-time run charts are made publicly available via the Crown web-tool and updated every 15 minutes. The run charts represent data in arrears of a month to account for higher data accuracy and to allow time for data entry activities.

Imperial publishes research findings using the aggregated data. Small numbers are suppressed throughout.

Stage 7 (third party applicants): ICL transfer anonymised, aggregated data onto third party once application has been approved by HQIP and RCP. If application requires it, Crown, NHS England and DHCW (and is granted following application to DARS for latter three) patient level audit data is sent to third party. Third party analyse this data and publish their research findings. Small numbers are supressed throughout.

Adult asthma and COPD Web-tool users

Web-tool users (those who enter and sign-off the data) register themselves (legal basis = consent) on the web-tool. Details (including name, job title, email address, place of work and contact number) are kept on the NRAP web-tool and are accessible to the NRAP team for administrative purposes (chasing, communication activities, reporting etc.).

Secondary care – Children and young people (CYP) asthma – 19/CAG/0001

Legal basis:

- 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.
- Article 9 (2) (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.
- 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.

CYP_Data Flow_v2.0_Decembe

Stage 1 (data entry and pseudonymisation): Local sites (i.e. clinicians, members of the audit team) enter audit data (including patient identifiable data (PID)) for appropriate patients via a bespoke web-tool hosted by Crown Informatics (www.nrap.org.uk). From 31st July 2022, local sites must also ensure that children and young people with asthma within England who have a national data opt out preference set (by self/parent/guardian) from the CYPA audit are not included in the data submitted to NRAP.

Crown anonymises data (audit and linked). NHS number is pseudonymised into audit ID, date of birth transformed to age, date of death is transformed into survival at x days and postcode is reduced to the first 4 digits (LSOA).

Stage 2 (audit data analysis and management): Pseudonymised patient level data is sent to ICL for data cleaning and analysis.

Stage 3 (report writing): Aggregated data is sent to RCP to draft audit outputs (e.g. national reports).

Stage 4 (linkage): Crown sends identifiable data to NHS England and DHCW for linkage purposes and CYP asthma data is combined with HES, PEDW and ONS and then pseudonymised by NHS England and DHCW. All patient level pseudonymised linked data is returned to ICL. ICL will combine the validated identifiers, NHS England and DHCW data and the relevant audit data and carry out data cleaning and analysis activities.

Stage 5 (linked data analysis and management): Following the cleaning and analysis of data by ICL, aggregated (i.e. analysed and non-identifiable) data will also be transferred from ICL to the RCP to provide commentary for, and then publish, outcome-related audit programme outputs (e.g. national reports, all data files etc).

Stage 6 (outcome report writing): Aggregated data is sent to RCP to draft audit outputs (e.g. national reports).

Hospital level real-time run charts are made publicly available via the Crown web-tool and updated every 15 minutes. The run charts represent data in arrears of a month to account for higher data accuracy and to allow time for data entry activities.

Imperial publishes research findings using the aggregated data. Small numbers are suppressed throughout.

Stage 7 (third party applicants): ICL transfer anonymised, aggregated data onto third party once application has been approved by HQIP and RCP. If application requires it, Crown, NHS England and DHCW (and is granted following application to DARS for latter three) patient level audit data is sent to third party. Third party analyse this data and publish their research findings. Small numbers are supressed throughout.

CYP asthma Web-tool users

Web-tool users (those who enter and sign-off the data) register themselves (legal basis = consent) on the web-tool. Details (including name, job title, email address, place of work and contact number) are kept on the NRAP web-tool and are accessible to the NRAP team for administrative purposes (chasing, communication activities, reporting etc.).

The section 251 approval for CYP asthma does not include the use of data for third-party applications.

Pulmonary rehabilitation (PR) – 23/CAG/0167

Legal basis:

- 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.
- Article 9 (2) (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

  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.

PR_Data Flow_v3.0 December 2024.pdf

Stage 1 (data entry and pseudonymisation): Local sites (i.e. clinicians, members of the audit team) enter audit data (including patient identifiable data (PID)) for appropriate patients via a bespoke web-tool hosted by Crown Informatics (www.nrap.org.uk). From 01 April 2024, local services must also ensure that adults enrolled for pulmonary rehabilitation within England who have a national data opt out preference set from the audit are not included in the data submitted to NRAP.

Crown anonymises data (audit and linked). NHS number is pseudonymised into audit ID, date of birth transformed to age and postcode is reduced to the first 4 digits (LSOA).

Stage 2 (audit data analysis and management): Pseudonymised patient level data is sent to ICL for data cleaning and analysis.

Stage 3 (report writing): Aggregated data is sent to RCP to draft audit outputs (e.g. national reports).

Hospital level real-time run charts are made publicly available via the Crown web-tool and updated every 15 minutes. The run charts represent data in arrears of a month to account for higher data accuracy and to allow time for data entry activities.

Imperial publishes research findings using the aggregated data. Small numbers are suppressed throughout.

Stage 4 (third party applicants): ICL transfer anonymised, aggregated data on to third party once application has been approved by HQIP and RCP. If application requires it, Crown, NHS England and DHCW (and is granted following application to DARS for latter three) patient level audit data is sent to third party. Third party analyse this data and publish their research findings. Small numbers are supressed throughout.

PR Web-tool users

Web-tool users (those who enter and sign-off the data) register themselves (legal basis = consent) on the web-tool. Details (including name, job title, email address, place of work and contact number) are kept on the NRAP web-tool and are accessible to the NRAP team for administrative purposes (chasing, communication activities, reporting etc.).

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 data is transferred outside of the EEA.

Privacy Risk Register
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/A	
NHS number (England and Wales)	Yes		Enables linkage with externally held national datasets for exploration of patient outcomes (readmissions and mortality). Also ensures automated duplicate checks can be carried out (i.e. within the web-tool). NHS number, postcode and date of birth are all collected for triangulation purposes. They enable the linkage service to link the correct data in a situation where one of the identifiers might be incorrect.
Address		N/A	
Postcode	Yes		As above and also enables exploration of social and economic deprivation (using Index of Multiple Deprivation (IMD) and Welsh Index of Multiple Deprivation (WIMD)). NHS number, postcode and date of birth are all collected for triangulation purposes. They enable the linkage service to link the correct data in a situation where one of the identifiers might be incorrect.
Date of birth	Yes		As above and also enables exploration of equity of care (i.e. whether different cohorts of patients – in this case patients of different ages - receive the same level of, and access to, care). NHS number, postcode and date of birth are all collected for triangulation purposes. They enable the linkage service to link the correct data in a situation where one of the identifiers might be incorrect.
Date of death	Yes		Where applicable, it is collected to ascertain the extent to which the patient's care impacts upon the key outcome of mortality.
Age		No	We collect date of birth and compute age using in-built web-tool validations.

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]*
Sex	Yes		The primary care report collects sex. This enables exploration of equity of care, i.e. whether different cohorts of patients receive the same level of, and access to care.
Marital Status		N/A	
Gender	Yes		Enables exploration of equity of care (i.e. whether different cohorts of patients receive the same level of, and access to, care).
Living Habits	Yes		Information on smoking and exposure to second-hand smoke are collected as they are key contributing factors in the care and management of COPD and asthma patients.
Professional Training / Awards		N/A	
Income / Financial / Tax Situation		N/A	
Email Address		N/A	
Physical Description		N/A	
General Identifier e.g. Hospital No		No	
Home Phone Number		N/A	
Online Identifier e.g. IP Address/Event Logs	Yes		Collected for users of the web-tool (i.e. not the patients that make up the audit cohort) due to the make-up of the NRAP web-tool (how the equipment needs to work with the internet) but this information is not accessed or used in anyway.
Website Cookies		N/A	
Mobile Phone / Device No		N/A	
Device Mobile Phone / Device IMEI No		N/A	
Location Data (Travel / GPS / GSM Data)		N/A	
Device MAC Address (Wireless Network Interface)		N/A	
Sensitive Personal Data			
Physical / Mental Health or Condition	Yes		Enables exploration of equity of care and parity of esteem (i.e. whether patients with different co-morbidities receive care of different standards). This will be: • extracted for the Primary Care audit, • obtained via linkage to HES and PEDW for the asthma audits and COPD audits
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	

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]*
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		As of 01 June 2023, all secondary care audits collect patient ethnic background to enable assessment of equity of care across race and ethnic origin.
Biometric Data (Fingerprints / Facial Recognition)		N/A	
Genetic Data		N/A	
Spare			
Spare			
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.

Streamlining of datasets will help minimise data entry omissions. Comprehensive validation rules are built into the web-tool to ensure that incorrect, conflicting and/or illogical data cannot be saved. Pop-up warnings appear for values that are plausible, but rare.

Comprehensive help notes for each question will be provided and the questions themselves reviewed annually to ensure they are clear. The central team will operate a helpdesk to answer queries that arise. FAQ documents will be available for all audits. Once data entry periods have closed, data will be exported and checked centrally for any inappropriate cases or illogical data before analysis.

For the primary care audit, robust rules will be applied to data cleaning to ensure that erroneous values are removed prior to analysis.

Details of registered webtool users will be audited periodically to ensure that we do not have out of date details. People who have signed up for information/newsletters will be contacted annually to ensure that they wish to remain on the distribution list.

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.	**Audit data** A privacy notice is available covering the whole programme. Fair processing notices are available for each audit component on the NRAP webpages. Posters and patient information leaflets are made available at all necessary healthcare services (primary, secondary care and PR) to ensure patients are aware of their data being used and for what purpose. **Web-tool users** Web-tool users voluntarily register themselves on the web-tool and are clear on the purposes for which	**Audit data** All (privacy notice, fair processing notices, posters and patient information leaflets) are available via the NRAP webpages (https://www.rcplondon.ac.uk/projects/information-governance) and Posters are sent to all GP practices and hospitals and patient information leaflets made available via URL. Posters and leaflets are also made available via the webpages (https://www.rcplondon.ac.uk/projects/patient-involvement-and-support). Where necessary, patient information leaflets have been made available for different age ranges and groups (for example adults, children (4-7 years and 8+ years) and parents so all necessary people have access to this information.	**Audit data** **Example – Link to full secondary care COPD fair processing notice.** https://www.rcp.ac.uk/projects/outputs/support-service-teams-copd **Web-tool users/contacts** Upon registering new users receive an automated email to inform them that their registration request will be shared with the approver for their service (often a clinical lead) as part of one of the web-tool security measures.

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
	their information will be used by the NRAP team (administrative only). This is done via: • Automated emails during the registration process • NRAP fair processing and privacy policies • Crown privacy policies	**Web-tool users** Web-tool users voluntarily register themselves on the web-tool and are clear on the purposes for which their information will be used by the NRAP team (administrative only). Automated emails are sent at different points during the registration process to keep new users up to date. User details are not used outside of programme administrative activities (chasing and audit communication).	
Individuals can access information held about them	This is included in the privacy notice Identifiable information is not accessible by the audit team but is available to key personnel at Crown Informatics. All access requests will be directed to Crown Informatics once received at the audit helpdesk. This does not apply to the primary care audit where the data is anonymised at source.	We would not be able to provide the information held but would put the person in touch with Crown Informatics who would be able to help.	Privacy Notice: *The right of access* You have the right to see what information is held about you. Crown Informatics are the only organisation in the clinical audit programme that receives personal data and this is anonymised as soon as possible. If you are a patient, we don't use names and addresses so you would have to know your NHS number. Once the data has been anonymised it would not be possible to identify if you were included in the audit sample. You have the *right to rectify* any data that is incorrect but rectifying it with us would not change the information in your health record and you may want to contact your healthcare provider directly.

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
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	This is included in the privacy notice **Audit data** All fair processing information and patient information leaflets provide individuals with the right to have their information removed from or not included in the audit. The section in the patient information is called 'Saying no thank you'. **Web-tool users** NRAP web-tool users can request that their information is removed from the web-tool as and when necessary. They can either do this via their own account or make a request via the NRAP helpdesk which is then communicated to Crown.	**Audit data** Fair processing information, posters and patient information leaflets as the different audit components launch – audit materials will not be available prior to this. Can be accessed via the NRAP webpages (www.nrap.org.uk) and via the necessary healthcare services (GP practice, hospitals or PR service). **Web-tool users** User account deletion/ modification information can be accessed by logged-in users via the NRAP web-tool (www.nrap.org.uk).	Privacy notice: *The right to erasure* You can request that we don't use personal information about you in our studies and we will ensure that any of your information we hold is destroyed. This will need to be done on a study by study basis otherwise the only way we could remove you from all studies would be to hold personal data about you to compare with the patient information that we receive. You also have the right to restriction of processing and to object to processing. We treat these the same way as the right to erasure and remove all information about you. If you decide that you would prefer that your information is not used please let us know by contacting us in writing at the postal address or use this email: nrapinbox@rcp.ac.uk **Audit data** **Example from the secondary care children and young people asthma fair processing information** ***Saying 'no thank you'*** In England, patients who have chosen to opt out of their confidential data being used for purposes other than their own care and treatment (National Data Opt-out Programme) will not be included in this audit. Wales does not operate a national data opt-out programme, but patients are still able to opt out of individual audits, such as this one. National clinical audit works best when it includes information about as many patients as possible. Patients should speak to a member of their clinical team if they do not want their information to be included. Saying this will not affect the care or

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
			treatment they receive in any way. Healthcare services should then ensure their information is not included in the audit and should note this for the future on their patient database. If a patient thinks their information has been submitted to the audit and they would prefer to have it removed, they should contact the hospital where they were treated or the audit team. **Web-tool users/contacts** User account deletion modification information can be found via the NRAP web-tool (www.nrap.org.uk). They can either do this via their own account or make a request via the NRAP helpdesk which is then communicated to Crown. **Patient information from the webtool**: Crown has ability to search by identifier and delete with permanency. Obtained from Crown System Level Security Policy (SLSP) 13.2 Data Disposal When the system or its data has completed or is no longer needed, the following methods will be adopted to dispose of equipment, back-up media or other stored data: • Disposal/erasing of data will be performed in accordance with any regulations or legislative requirements, but information will be wiped from all digital media using a recognised erasing tool to ensure that data is not recoverable. • Data no longer required will be erased from the system and the space reused. • Back-up tapes will be overwritten or destroyed. • If the machine is no longer required, the data storage drives will be removed and physically destroyed and the

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
			remaining components will be disposed of.
Rectification of inaccurate information	This is included in the privacy notice	We can rectify inaccurate information but would recommend that people contact the health provider that supplied the information to rectify at source.	Privacy Notice: *The right to access* You have the right to see what information is held about you. Crown Informatics are the only organisation in the clinical audit programme that receives personal data and this is anonymised as soon as possible. If you are a patient, we don't use names and addresses so you would have to know your NHS number. Once the data has been anonymised it would not be possible to identify if you were included in the audit sample. You have the *right to rectify* any data that is incorrect but rectifying it with us would not change the information in your health record and you may want to contact your healthcare provider directly.
Restriction of some processing	This is included in the privacy notice **Audit data** All fair processing information and patient information leaflets provide individuals with the right to have their information removed from or not included in the audit. The section in the patient information is called 'Saying no thank you'. **Web-tool users** NRAP web-tool users can request that their information is removed from the	**Audit data** Fair processing information, posters and patient information leaflets. These can be accessed via the NRAP webpages (www.nrap.org.uk) and via the necessary healthcare services (GP practice, hospitals or PR service). **Web-tool users** User account deletion/ modification information can be accessed by logged-in users via the NRAP web-tool (www.nrap.org.uk).	Privacy notice: *The right to erasure* You also have the right to restriction of processing and to object to processing. We treat these the same way as the right to erasure and remove all information about you. All existing and future fair processing (including privacy notices) and patient information does or will include details of how patients can have their information removed or not included in the audits. **NRAP web-tool user** NRAP web-tool users can request that their information is updated from the web-tool/changed as and when necessary. They can either do this via their own account or make a request via the NRAP helpdesk which is then communicated to Crown.

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
	web-tool as and when necessary. They can either do this via their own account or make a request via the NRAP helpdesk which is then communicated to Crown.		
Object to processing undertaken on some legal bases	This is included in the privacy notice **Audit data** There is a National Data Opt-Out Programme (NDO) which runs in England and enables patients residing or being treated in England to apply a blanket 'opt-out' to their identifiable healthcare data being used for secondary purposes (such as audit and research). All fair processing information and patient information leaflets provide individuals with the relevant information on how to have their information removed from or not included in the audit. The section in the patient information is called 'Saying no thank you'.	**Audit data** Fair processing information, posters and patient information leaflets via the NRAP webpages (www.nrap.org.uk) and via the necessary healthcare services (GP practice, hospitals or PR service). See information to the left on how the objection is applied for each of the different countries (England and Wales).	Privacy notice: *The right to erasure* You also have the right to restriction of processing and to object to processing. We treat these the same way as the right to erasure and remove all information about you. All NRAP documentation explains the National Data Opt-Out Programme (NDO) for all continuous audit workstreams (AA, CYP, COPD and PR) in England and how this differs to how objections are applied for Wales (and individual opt-outs in England). In addition, the information makes it clear that for Wales objecting to one audit component does not automatically remove them from another of the NRAP audits. They can, therefore, object to one audit but still be included in others. The NDO does not apply to the Primary Care workstream. **Audit data** **Example from the secondary care adult asthma fair processing information** ***Saying 'no thank you'*** In England, patients who have chosen to opt out of their confidential data being used for purposes other than their own care and treatment (National Data Opt-out Programme) will not be included in this audit. Wales does not operate a national data opt-out programme, but patients are

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
			still able to opt out of individual audits, such as this one. National clinical audit works best when it includes information about as many patients as possible. Patients should speak to a member of their clinical team if they do not want their information to be included. Saying this will not affect the care or treatment they receive in any way. Healthcare services should then ensure their information is not included in the audit and should note this for the future on their patient database. If a patient thinks their information has been submitted to the audit and they would prefer to have it removed, they should contact the hospital where they were treated or the audit team.
Complain to the Information Commissioner's Office;	This is included in the privacy notice	Contact details for the ICO are provided.	**Contact the Information Commissioner's Office** If you are unhappy with the way we handle your data or have dealt with a request, you have the right to lodge a complaint with the Information Commissioner's Office at https://ico.org.uk/concerns or telephone 0303 123 1113.
Withdraw consent at any time (if processing is based on consent)	This is included in the privacy notice **NRAP web-tool users** NRAP web-tool users can request that their information is removed from the web-tool as and when necessary. They can either do this via their own account or make a request via the NRAP helpdesk which is	**Audit data** Fair processing information which is available via the NRAP webpages (www.rcp.ac.uk/nrap). **NRAP web-tool users** User account deletion/ modification information can be accessed by logged-in users via the NRAP web-tool (www.nrap.org.uk).	Privacy notice: *Consent* Where people sign up to receive newsletters and updates, attend events or work with NRAP, consent is received for us to store and process personal data. **NRAP web-tool user** NRAP web-tool users can request that their information is deleted from the web-tool as and when necessary. They can either do this via their own account or make a request via the NRAP helpdesk which is then communicated to Crown.

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
	then communicated to Crown.		
Data portability (if relevant)	This is included in the privacy notice	N/A	Privacy notice: *The right to data portability* If we do have information held about you and you wish to see it, we will provide your data in a format that you will be able to use, such as Microsoft Word, Excel or CSV.
Individual knows the identity and contact details of the data controller and the data controllers data protection officer	**Audit data** This information is given within all fair processing notices. **NRAP web-tool users** Information on the identity and contact details of the data controller and their data protection officers can be found within the NRAP web-tool information.	**Audit data** Fair processing notices are available via the NRAP webpages (www.rcp.ac.uk/nrap) **NRAP web-tool users** User account deletion/ modification information can be accessed by logged-in users via the NRAP web-tool (www.nrap.org.uk).	**Audit data** **Example from secondary COPD audit fair processing information** *The Healthcare Quality Improvement Partnership (HQIP) are the data controllers for all data collected and reported on by the National Respiratory Audit Programme. All data collected by the audit programme is processed to ensure patient confidentiality is maintained.* **NRAP web-tool user** Information from the NRAP web-tool for users. The programme has been commissioned by the (HQIP) as part of the National Clinical Audit and Patient Outcomes Programme (NCAPOP) and currently covers England and Wales only. The audit programme is led by the Royal College of Physicians (RCP). For more information on the National Respiratory Audit Programme please visit: www.rcp.ac.uk/nrap.
In which countries the data controller is processing their personal data. For data transfers outside the EU, a description of how the data will	N/A	N/A	N/A

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
protected (e.g. the recipient is in an 'adequate' country / how a copy of the safeguards can be obtained.			
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?	This is included in the privacy notice, fair processing notices and the patient information leaflets.	Both the fair processing notices and patient information leaflets for each audit component can be found via the NRAP webpages (https://www.rcplondon.ac.uk/projects/patient-involvement-and-support). Patient information leaflets are also made available via a URL in the posters.	**Example from the adult asthma clinical audit patient information leaflet** ***Why haven't hospital staff asked for permission to use my information?*** *This audit has special legal permission to collect confidential information without patient consent, with the exception of where a national data opt-out is set. This is because it can be difficult to ask patients when they have an asthma attack. Some patients may find it hard to communicate and some won't have relatives with them who can communicate their preference on their behalf. An asthma attack is a very distressing time for patients and asking them about the audit at this time would not be the most important priority.* **Example from COPD fair processing notice** This audit has been granted Section 251 approval for England and Wales by the NHS Health Research Authority (CAG reference number: 23/CAG/0045), meaning that we are allowed to collect patient-identifiable data without patient consent. • The COPD audit collects the following patient identifiable items: o NHS number; o date of birth; o home postcode; o date of death (if death occurred during admission). *More information about the audit data flows (also outlined below) and the full dataset is*

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
			available via the support for services page. Patient information sheets and posters are also available via the Downloads page of the audit web tool. **Example from the primary care patient information leaflet** ***Permission and data safety*** Your information will be used in a way that ensures that you cannot be identified. Your permission is not needed for this audit. Organisations handling your data must follow laws to keep your information safe. ***How is the information used?*** GP surgeries will receive reports to improve your care. Reports also help identify areas requiring improvement across Wales. The data may be used for research; your identity is always protected. ***Saying 'no thank you'*** In the past, patients could say 'no' or 'opt out' of allowing their data to be used for audit. As only anonymous data is used, this is now not applicable. From the Privacy Notice: **Our legal basis for collecting information** The legal bases for collecting and using personal data are: *Public Task* We collect only the information that is necessary to carry out our function and avoid collecting information that will not be used. This is received from healthcare providers, such as NHS Trusts and Health Boards. To see what information is held in your healthcare record please contact your local Trust or Board. Article 6 • 1 (e) - processing is necessary for the performance of a task carried out in the public interest or in the

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
			exercise of official authority vested in the controller. *Consent* Where people sign up to receive newsletters and updates, attend events or work with NRAP consent is received for us to store and process personal data. *Contract* For example, this is the basis we use when it is necessary for us to take specific steps before entering into a contract with you to supply you a service or vice versa. *Legal obligation* For example, this is the basis we use when it is necessary for us to comply with the law (not including contractual obligations) because we are required to keep documentation to produce in court proceedings. *Legitimate interests* This basis is used to allow us to hold information as evidence should we need it in the future, for example, if you ask us to unsubscribe you from our newsletter. *Common Law Duty of Confidentiality* We apply the Common Law Duty of Confidentiality to all data we hold. Article 9 condition for processing special category data: 2 (h) - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3. • 2(i) - processing is necessary for reasons of public interest in the area of public

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
			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.
To know the purpose(s) for the processing of their information.	This is included in the privacy notice, the fair processing notices and patient information leaflets include information on this.	The fair processing notices, privacy notice and patient information leaflets for each audit component can be found via the NRAP webpages (www.rcp.ac.uk/nrap). Patient information leaflets are also made available via a URL in the posters.	**Example from adult asthma clinical audit patient information leaflet** The information collected will show which parts of asthma care are good and which parts need improving. The audit will also help to make sure that information on the quality of care is available to the public. From the privacy notice: **How and why we use the information** The primary purpose of NRAP's work is to investigate the quality of care provided to patients in order to improve the care of future patients. Direct or ongoing individual patient care will not be affected. All patients who meet the criteria we are looking at, such as children and young people with asthma who have been in contact with hospital services during the audit period, will be entered into the online data collection tool. If a patient has chosen to opt-out of their data being used for any purposes other than their healthcare, they will be removed from the sample by the hospital submitting the data. Only date of birth and NHS number and postcode are collected along with non-identifiable information about their care. Patient-identifiable information is collected without obtaining consent from the patient under Section 251 of the NHS Act 2006 in England and Wales, given by the Health Research Authority. This allows us to breach the Common Law Duty of Confidentiality by collecting personal data

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
			under specific circumstances and with strict data security procedures in place. The anonymised and analysed data is kept for 5 years, in line with the Information Governance Alliance's Records Management Code of Practice for Health and Social Care 2016.
Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the personal data.	N/A	N/A	N/A
The source of the data (where the data were not collected from the data subject)	The patient information leaflets provide this information.	Patient information leaflets are made available via URL (in the posters) and PDF on the NRAP webpages (www.rcp.ac.uk/nrap)	**Example from adult asthma clinical audit patient information leaflet** ***Where does my confidential information go?*** Hospitals taking part in this audit enter the information, or data, they collect about patients and their care into an online database called a 'web-tool'. The data will be held there for the duration of the audit and then for a further 5 years. The data are held by an organisation called Crown Informatics which created the audit web-tool. Staff at Crown Informatics may see your personal details, such as NHS number, postcode, gender and ethnicity as part of database administration. Crown Informatics will take the data that are inputted by hospitals, remove information that would enable you to be identified and send it to Imperial College London, who analyse the data. They then send results of the analysis to the NRAP team to produce

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
			reports. The NRAP team cannot see information on individual patients. Periodically, Crown Informatics will also send your data to a number of organisations in England and Wales to link to other sources. They send your NHS number, date of birth and postcode data to NHS England and DHCW (Digital Health and Care Wales). NHS England has a record of all hospital admissions from the Hospital Episode Statistics (HES) dataset in England. DHCW holds this data from the Patient Episode Database for Wales (PEDW). HES and PEDW will be linked to the audit data. NHS England will also provide date and cause of death data from the civil registration records on behalf of the Office for National Statistics (ONS) for England and Wales. The 'linked' data will then have the confidential information removed by NHS England and DHCW. The 'linked' data are then sent to Imperial College London, to be processed, analysed and aggregated. The results are then shared with the NRAP team to produce outcome reports. A graphical representation of the 'data flow' can be found on our website at https://www.rcplondon.ac.uk/projects/outputs/support-service-teams-adult-asthma
Categories of data being processed	Datasets and data flows.	Audit datasets and data flows are available on the NRAP webtool (www.rcp.ac.uk/nrap). Data flows are colour coded to enable easy identification of what category of information each flow falls into (identifiable, anonymised, anonymised and aggregated).	Please note the following: COPD, adult and children and young people asthma, PR and primary care audit information are available at www.rcp.ac.uk/nrap. Information will include datasets and data flows which will outline all categories of data being processed by NRAP.

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
Recipients or categories of recipients	Datasets and data flows.	Data flows are available on the NRAP webpages (www.rcp.ac.uk/nrap). All data flows include information on data processes and controllers for each stage of the process.	COPD, adult and children and young people asthma, pulmonary rehabilitation and primary care audit information are available at www.rcp.ac.uk/nrap. Information includes data flows which will outline all recipients or categories of recipients who receive audit data.
The source of the personal data	The privacy notice and patient information leaflets provide this information.	Patient information leaflets are made available via URL (in the posters) and PDF on the NRAP webpages (www.rcp.ac.uk/nrap)	**Example from adult asthma clinical audit patient information leaflet** ***Where does my confidential information go?*** Hospitals taking part in this audit enter the information, or data, they collect about patients and their care into an online database called a 'web-tool'. The data will be held there for the duration of the audit and then for a further 5 years. The data are held by an organisation called Crown Informatics which created the audit web-tool. Staff at Crown Informatics may see your personal details, such as NHS number, postcode, gender and ethnicity as part of database administration. Crown Informatics will take the data that are inputted by hospitals, remove information that would enable you to be identified and send it to Imperial College London, who analyse the data. They then send results of the analysis to the NRAP team to produce reports. The NRAP team cannot see information on individual patients. Periodically, Crown Informatics will also send your data to a number of organisations in England and Wales to link to other sources. They send your NHS number, date of birth and postcode data to NHS England and DHCW (Digital Health and Care Wales). NHS England has a record of all hospital admissions from the Hospital Episode Statistics (HES) dataset in England. DHCW holds this data from the Patient Episode Database for Wales (PEDW). HES

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
			and PEDW will be linked to the audit data. NHS England will also provide date and cause of death data from the civil registration records on behalf of the Office for National Statistics (ONS) for England and Wales. The 'linked' data will then have the confidential information removed by NHS England and DHCW. The 'linked' data are then sent to Imperial College London, to be processed, analysed and aggregated. The results are then shared with the NRAP team to produce outcome reports. A graphical representation of the 'data flow' can be found on our website at https://www.rcplondon.ac.uk/projects/outputs/support-service-teams-adult-asthma **Example from the privacy notice:** The audit information will be linked with data already held by NHS England and Digital Health and Care Wales (DHCW): namely, the Hospital Episodes Statistics (HES) and Patient Episode Database for Wales (PEDW) datasets and the Office for National Statistics (ONS) mortality data.
To know the period for which their data will be stored (or the criteria used to determine that period)	As above	As above	As above
The existence of, and an explanation of the logic involved in, any automated processing that	N/A	N/A	N/A

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
has a significant effect on data subjects (if 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.

Secondary care components
All patients admitted to hospital with an acute exacerbation of COPD or an acute asthma attack are included in the scope of the audit.

COPD
There are currently over 534,000 COPD clinical records on the NRAP webtool. There are an estimated 115,000 admissions to hospital as a result of COPD each year. The aim is for 100% case ascertainment, therefore, we would hope the dataset would increase by approximately 115,000 per annum. There were 67,963 patients entered into the COPD audit during the period 01 April 2023 to 31 March 2024.

Adult Asthma
There are currently over 111,000 adult asthma exacerbation records on the NRAP webtool. Approximately 60,000 people (adult and children and young people) are admitted to hospitals for acute asthma attacks each year. The aim will be for 100% case ascertainment. There were 20,031 patients entered into the adult asthma audit during the period 01 April 2023 to 31 March 2024.

Children and Young People Asthma
There are currently over 69,000 children and young people asthma exacerbation records on the NRAP webtool. Approximately 60,000 people (adult and children and young people) are admitted to hospitals for acute asthma attacks each year. The aim will be for 100% case ascertainment. There were 14,789 patients entered into the adult asthma audit during the period 01 April 2023 to 31 March 2024.

Pulmonary rehabilitation (PR) component
There are currently over 142,000 PR patient records on the NRAP webtool. There are approximately 46,000 COPD patients assessed for PR per year although estimates for the audit are 30,000 per year (65% case ascertainment). There were 31,846 patients entered into the pulmonary rehabilitation audit during the period 01 April 2023 to 31 March 2024. As of 01 November 2023, the PR audit expanded to include patients who are referred for pulmonary rehabilitation with the following patient primary disease - COPD, asthma, bronchiectasis, interstitial lung disease, long covid, other chronic respiratory disease, pre/post thoracic surgery (including lung cancer/LVR/lung transplant), pulmonary hypertension, chronic heart failure. A recently conducted service survey advised that this expansion could potentially triple eligible patients.

Table continued:

Primary care component

The 2017 primary care audit was conducted on COPD patients only. This audit captured 82,696 COPD patient records in this audit cycle. There are 260,000 people in Wales with asthma and the successive audit cycles from 2018 was conducted for both patients with asthma and COPD. The audit captured 148,933 patient records in 2017/18 audit cycle, 189,149 records in the 2020 audit cycle and 127,159 patient records in the 2021 audit cycle. The 2021 audit was conducted on COPD and asthma patients. The audit captured 32,275 patients with COPD, 84,583 adults with asthma and 10,301 children with asthma. In 2021, 314 general practices took part in the audit out of a possible 389. In the 2021-23 cohort, 359 practices in Wales took part in the audit out of a possible 375. This captured 83,529 patients with COPD, 175,752 adults with asthma and 24,214 children and young people with asthma between 1st August 2021 and 31st July 2023.

Webtool user component

There are currently **over** 6200 unique users/contacts currently registered on the NRAP webtool.

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	1	5	5	**Accepted**	Crown Informatics Ltd holds all identifiable information on behalf of NRAP. The NRAP team/other sub-contractors do not have access to these identifiers. **Data security at Crown** (web-tool in use for secondary care). Only nominated individuals have access to the data, and only the individual units themselves can see the patient identifiable data of their own patients. Access to data is via secure client software, operating over secure VPN firewalled networks using secondary application layer security	**Crown** have an excellent reputation for data security. Their security systems ensure that all data is held safely and the risk of breach is an absolute minimum. Annual checking of DSPT is undertaken by the programme	Continuous through lifetime of contract	Programme manager at sub-contract review meetings

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
					provided by IBM. Data is stored and processed at a secure data centre; this operates to ISO 27001 certification (2015). **Data security at Imperial College London** (only have pseudonymised data) Primary care data: On an encrypted hard drive locked in a safe which is bolted to the wall. Secondary care and pulmonary rehabilitation data: On a password protected computer on an encrypted internal hard drive which sits in a locked room. The datasheets themselves are also password protected	**Imperial College London** takes all necessary measures to ensure that the data they hold is secure and inaccessible to anyone not authorised to access it. Annual checking of DSPT is undertaken by the programme		

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
					individually as well as the computer. Data is regularly backed up on a server, and access to servers are certified to ISA 7001, the recognised standard for data security.			
Undesired modification	1	4	4	**Accepted**	As above	As above	Continuous through lifetime of contract	Programme manager at sub-contract review meetings
Disappearance of data	1	3	3	**Accepted**	**Crown Informatics Ltd** sub-contract who hold all patient level and identifiable information. Backups are encrypted at AES256, held in dual copies, and stored securely. As above for **Imperial College London**.	**Crown** have an excellent reputation for data security. Their security systems ensure that all data is held safely and the risk of	Continuous through lifetime of contract	Programme manager at sub-contract review meetings

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
						disappearance or loss of information is at an absolute minimum. **Imperial College London** take all necessary measures to ensure that the data they hold is secure and inaccessible to anyone not authorised to access it. All data is backed up on an secure server.		

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
Network failure (RCP)	1	5	5	**Accepted**	**Data security at RCP.** Data is regularly backed up on a server, and access to both servers are certified to ISA 7001. This will ensure that despite a network failure access can still be gained to key information.	This ensures that even if a network failure is experienced all information remains safe and unharmed.	Continuous through lifetime of contract	Programme manager / IG lead
Sub-contractor network failure or cyber-attack	1	5	5	**Accepted**	**Crown Informatics Ltd** holds all identifiable information on behalf of NRAP. The NRAP team and all other sub-contractors do not have access to this. Data security at Crown (web-tool in use for secondary care). Only nominated individuals have access to the data, and only the individual units themselves can see the	**Crown** have an excellent reputation for data security. Their security systems ensure that all data is held safely and the risk of breach is an absolute minimum. All	Continuous through lifetime of contract	Programme manager at sub-contract review meetings

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**
					patient identifiable data of their own patients. Access to data is via secure client software, operating over secure VPN firewalled networks using secondary application layer security provided by IBM. Data is stored and processed at a secure data centre; this operates to ISO 27001 certification (2015). Backups are encrypted at AES256, held in dual copies, and stored securely. As above for Imperial College London.	the necessary fire walls and precautions are in place to deal with and avoid with cyber events. **Imperial College London** take all necessary measures to ensure that the data they hold is secure and inaccessible to anyone not authorised to access it. All data is backed		

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
						up on a secure server.		
Data breach	2	3	6	**Reduced**	The audit programme is subject to comprehensive data regulations, and will do the following to both reduce and transfer the risk of a data breach: - Legal basis. The audit programme will ensure that the secondary care audits and pulmonary rehabilitation audit are covered under Section 251 of the Health and Social Care Act (reference: 23/CAG/0045, 19/CAG/0001 and 23/CAG/0167). - Data security at Crown (web-tool in use for secondary care). Only nominated individuals have access to the data, and only the individual units	These measures ensure that the risk of a data breach is extremely low. They ensure the security of all information (identifiable and anonymised).	Continuous through lifetime of contract	Programme manager – check at sub-contract review meetings

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**
					themselves can see the patient identifiable data of their own patients. Access to data is via secure client software, operating over secure VPN firewalled networks using secondary application layer security provided by IBM. Data is stored and processed at a secure data centre; this operates to ISO 27001 certification (2015). Backups are encrypted at AES256, held in dual copies, and stored securely. Data security at RCP and ICL. Data is regularly backed up on a server, and access to both servers are certified to ISA			

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**
					7001, the recognised standard for data security. - All members of the audit team have data protection training on an annual basis. *Removal of data if requested by a patient* Crown has ability to search by identifier and delete with permanency. Obtained from Crown System Level Security Policy (SLSP) When the system or its data has completed or is no longer needed, the following methods will be adopted to dispose of equipment, back-up media or other stored data:			

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**
					• Disposal/erasing of data will be performed in accordance with any regulations or legislative requirements, but information will be wiped from all digital media using a recognised erasing tool to ensure that data is not recoverable. • Data no longer required will be erased from the system and the space reused. • Back-up tapes will be overwritten or destroyed. • If the machine is no longer required, the data storage drives will be removed and physically			

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
					destroyed and the remaining components will be disposed of. Posters, patient information leaflets and fair processing information are made widely available to ensure that patients are aware of the audit and how and why their data is used. There is the option for them to ask for their information not to be included in the audit if they do not wish it to be.			

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**
Corporate risks & compliance risks section								
National Data Opt-out risk (England only)	2	3	6	**Accepted**	There is a risk that patients who have opted-out of having their patient identifiable information used for audit/research/planning purposes will be incorrectly entered onto the audit webtool. Other than ensuring that information on this is included in the audit guidance there is nothing the audit can do as it will not have access to the central spine repository where this information is held. Responsibility for not entering that patients' data is solely with the hospital/health and social care service who are		Continuous through lifetime of contract	Programme manager

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
					entering the data. This does not apply to Wales. NRAP and Crown are in regular discussions with HQIP regarding compliance and to ensure a consistent approach across the programme			
Section 251 annual reviews – not submitted	1	4	4	**Reduced**	The majority of the legal basis requirements involve an annual review of the approval – particularly section 251. There is a risk that these are delayed or not submitted and NRAPs legal basis is not valid for a time period. All senior programme staff (clinical leads, programme and project managers) are to have an awareness of these process and the dates that they are due. Reminders are placed in calendars and in project plans	With all senior team members knowing the details and dates of these that the likelihood of them being missed is significantly reduced.	Continuous through lifetime of contract	Programme manager / IG lead

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
					to ensure all necessary team members are aware of the requirement to update these essential documents and approvals.			

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	This was done via CQID senior management.
Name of DPO	Pamela Forde	
Name and role of person approving completion of DPIA form. This must not be the same person that completes the form.	Pamela Forde Royal College of Physicians Data Protection Officer	This was done via CQID senior management but no queries or concerns were raised on return.
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	Page 12
Does it include a systematic description of the proposed processing operation and its purpose?	Yes	See page 9-10
Does it include the nature, scope, context and purposes of the processing	Yes	See page 8-11
Does it include personal data, recipients and period for which the personal data will be stored are recorded	Yes	See page 8-11
Does it include the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels)	No	
Does the DPIA explain how each individual's rights are managed? See section on individuals rights	Yes	See pages 21-37
Are safeguards in place surrounding international transfer? See section on	N/A	

sending information outside the EEA		
Was consultation of the document carried out and with whom?	Yes	RCP Data protection officer CQID senior management NRAP programme manager NRAP web-tool provider NRAP data analysis lead
Organisations ICO registration number	Yes	See page 2
Organisations ICO registration expiry date	Yes	See page 2
Version number of the DPIA you are submitting	Yes	See page 2
Date completed	Yes	See page 2

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>
<tr><td>4</td><td>Major</td><td>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</td></tr>
<tr><td>5</td><td>Catastrophic</td><td>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</td></tr>
</table>
</td></tr>
</table>

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?