National Respiratory Audit Programme (NRAP)

Pulmonary Rehabilitation audit – Frequently asked questions (FAQs): Information governance

Version 4.0.3: March 2024

A general audit FAQ and a specific FAQ for National Data Opt-Out in the PR audit are available separately.

1. Who is involved in running the audit?

- The National Respiratory Audit Programme (NRAP) Pulmonary Rehabilitation (PR) audit is managed and operated by the **Royal College of Physicians, London (RCP)** in collaboration with:
    - **Healthcare Quality Improvement Partnership (HQIP)** – commission the audit and are **data controllers** for the audit.
    - **Crown Informatics** – provide the audit web tool and data management services.
    - **Imperial College London** – provide statistical data analysis services.

The RCP, Crown Informatics and Imperial College London are all **data processors.**

2. Has the audit got approval to collect identifiable information?

- The audit has Section 251 approval from the Health Research Authority's (HRAs) Confidentiality Advisory Group (CAG) to collect patient identifiable data (including NHS number, date of birth and postcode without obtaining patient consent (reference: 23/CAG/0167) for patients assessed for PR from 1 April 2024 onwards.
- A record of the approval can be found at https://www.hra.nhs.uk/planning-and-improving-research/application-summaries/confidentiality-advisory-group-registers/
- Each participating service's Caldicott Guardian must also provide written approval before any data can be entered.

3. What are PR services required to do?

a. **For patients assessed for PR from 1 April 2024 onwards:**

Although patients do not need to provide consent for inclusion in the audit (see response to question 2), PR services must carry out fair processing activities, including the following:

- Display the patient information poster in all areas where patients assessed for PR may be treated.
- If a patient asks for further information, direct them to the patient information leaflet online, or hand them a copy.

Copies of both the poster and patient information leaflet are available to download from the patient support page.

Patients in England must be screened through the National Data Opt-Out scheme before being entered into the audit. If any patient informs you that they do not wish to be included in the audit, please make this clear in the patient's notes and do not enter their data into the audit.

b. **For patients assessed for PR before 1 April 2024**

For patients assessed before 1 April 2024 only, services will need to manage a process of informed explicit consent. The procedure for patient consent is outlined below:

Audit lead responsibilities	**The audit lead must ensure there are clear and systematic processes in place so that their team is able to:** 1. Display the patient information poster in an appropriate location. 2. Provide patients with the patient information sheet. 3. Obtain written/verbal consent from patients (using the patient consent form). 4. Keep consent forms in accordance with Caldicott principles. 5. Keep a record of the number of patients who are asked to consent, and how many refuse consent (this information is needed for case ascertainment and workforce planning requests).

Staff Responsibilities	**No specific staff training is required to obtain consent, but service staff should do the following when obtaining consent:** 1. Provide each patient with a patient information sheet, provide an explanation of the audit, and give the patient the opportunity to ask questions. 2. Record consent from willing patients on the consent form provided. Please note, the patient will need to sign and initial the document to give consent. 3. For consent given verbally or over the phone, then 'V' should be inserted into the signature box in place of a physical signature from the patient. 4. Retain the signed patient consent form in the patient's notes (do **not** send completed forms or copies to the audit team). 5. Please feel free to provide patients with copies of their consent forms.
General Information	1. We recommend that patients are approached by a member of the PR service team to give their consent at their initial assessment/first appointment. If this is not possible, consent can be given at a later point during the programme, but **you must not input <u>any</u> data into the audit web tool before written consent has been obtained from the patient.** 2. If a patient does not wish to be included in the audit, please make this clear in the patient's notes and inform the audit lead. 3. If a patient initially gives consent but later withdraws it, please make this clear in the patient's notes, inform the audit lead, and contact the RCP audit team to arrange for any data to be deleted. Any withdrawal of consent must be communicated to the RCP before data is extracted for analysis – after this point, it will not be possible to locate and delete individual records. This is clearly explained in the patient information sheet.

4. What are the data flows?

- The PR data flows are publicly available on the PR audit webpages.
- Approved users at each registered service enter data into a bespoke web tool (www.nrap.org.uk) hosted by Crown Informatics.
- Data from each unit is only visible to authorised users within that hospital according to the audit profile and to Crown Informatics for web tool and data management purposes. Crown Informatics 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 (PID) 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 PID. 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 spot checks. Bulk access to PID is necessary to undertake linkage exercises (i.e. to prepare the files for transfer to NHS England or Data Health and Care Wales (DHCW)).
    - Subject access requests - when a patient requests their audit details.
- Non-identifiable patient level data is sent from Crown Informatics to Imperial College London for statistical analysis purposes.
- Following analysis, non-identifiable aggregated patient data is sent from Imperial College London to the audit team (at the Royal College of Physicians) for reporting purposes.
- Non- identifiable patient level data may also be shared with third-parties for research, audit and service evaluation under Data Sharing Agreements (DSAs), which are arrangements agreed separately as required according to IG recommendations.

5. Who has access to the data?

a. **Patient identifiable data**

- Only nominated individuals at each hospital and Crown Informatics can see any patient-related identifiable data. Access to data is carried out for necessary administrative purposes only by named, trained, and certified individuals.

- Crown Informatics has a Data Security and Protection Toolkit (DSPT) rating of Standards Exceeded (ODS code: 8J157) and meets all NHS guidelines and requirements.
- They are also registered with the Data Protection Authorities (DPA) under reference: Z3566445.
- Access to data is via secure client software that operates over secure encrypted firewalled networks using secondary application layer security.

b. **Non-identifiable patient data**

- Only members of the Imperial College London analysis team will have access to anonymised patient level data sent to them by Crown Informatics.
- Imperial College London has an DSPT (ODS code: EE133887-SPHTR) rating of Standards Met and meets all NHS guidelines and requirements.
- They are also registered with the Data Protection Authorities (DPA) under reference: Z5940050.
- Data Sharing and Transfer Agreements duly authorised by the audit commissioners (HQIP) will govern the transfer of non-identifiable patient data to any approved third parties.

c. **Anonymised and aggregated level data**

- Members of the NRAP team at the Royal College of Physicians receive anonymised and aggregated data from Imperial College London.
- The Royal College of Physicians has a DSPT (ODS code: 8J008-CSD) rating of Standards Met and meets all NHS guidelines and requirements.
- The Royal College of Physicians is also registered with the Data Protection Authorities (DPA) under reference: Z7085833.

6. How is data transferred?

- Data is collected over secure web/internet-based systems using high strength TLS (SSL) protocols (256 bit, SHA256 signatures and 4096 bit certificates).
- The web tool SSL certificate is ‘organisationally verified’ (OV) and issued by an established respected global certifier).
- Data is transferred to NHS England via their secure DSCRO system.

7. How and where is the data stored?

a. Crown Informatics

- Data is stored and processed at a secure UK-based ISO 27001 certified data centre.
- The servers are owned and operated by Crown Informatics and are held in a secure locked rack, accessible to named individuals. All access is logged, managed and supervised.
- Data is stored in secure encrypted databases.
- Backups are encrypted (AES256), held in dual copies, and stored securely.

b. Imperial College London

- Data is stored on a password-protected computer on an encrypted internal hard drive which sits in a locked room. Datasheets themselves are also password protected individually as well as the computer.
- Data is regularly backed up and access to servers is certified to ISO 27001.

8. What is the data retention schedule?

- Data will be retained for the duration of the audit in order to complete longitudinal analyses, including assessing long-term outcomes for the patients with respiratory conditions who attended PR.
- All data will be destroyed in line with Information Governance Alliance (IGA)'s Records Management Code of Practice for Health and Social Care (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 requires that clinical audit records must be kept securely for a period of 5 years after a National Respiratory Audit Programme audit has been completed. This will enable the RCP to answer any post-closure queries.
- This retention schedule has been approved by the CAG.

NRAP will be funded by HQIP until 31 May 2026, at which point a decision will be taken about the future of the work.