Policy Document

National Ophthalmology Database Audit: Information Governance

Date of issue	July 2024
Review date	July 2025
Approved by	Caroline Wilson 25 July 2024
Document Owner	Beth Barnes

The Royal College of Ophthalmologists
18 Stephenson Way, London, NW1 2HD | T. 020 3770 5347
noa.project@rcophth.ac.uk | nodaudit.org.uk | rcophth.ac.uk | @RCOphth

Contents

1. Introduction

1.1 Purpose and scope

This document outlines the Information Governance (IG) issues that impact the Royal College of Ophthalmologists' (RCOphth) National Ophthalmology Database (NOD) Audit and how these are managed. It is intended to inform Caldicott Guardians, Senior Information Risk Owners (SIRO) and Information Governance Officers participation decisions. It is also intended to demonstrate the NOD has been developed in accordance with best practice regarding Information Governance and is transparent on all aspects of IG and complies with statutory IG guidance.

The NOD currently runs two national clinical audits in the UK and Guernsey:

1. Adult cataract surgery covering key service and surgeon outcomes. Surgeons include consultants, SAS doctors and ophthalmologists in training
2. Age-related Macular degeneration services for people undergoing treatment for Late AMD. (See NICE Guideline NG82 https://www.nice.org.uk/guidance/ng82- Age-related macular degeneration February 2018 for definitions of Early and Late AMD).

1.2 Background

The NOD was developed under the auspices of The Royal College of Ophthalmologists in 2009. The aims were to develop a national resource for audit and research of eye diseases and to support the development of robust quality standards for revalidation of ophthalmologists. All data were collected as a by-product of routine clinical care using Electronic Medical Records (EMR) systems used in Hospital Eye Services.

The data sets for the NOD audits are accessed via the NOD Audit website,
https://nodaudit.org.uk/healthcare-professionals/audit-participation-and-access
The RCOphth is the content sponsor for the Cataract National Data Set. The data set was approved in April 2010 by the Information Standards Board (ISB) as an inherited information standard based on good evidence of its use a) in electronic cataract care records and b) to support national audit, benchmarking, research, and quality improvement. It is approved for use for those purposes within units providing cataract surgery. However, some amendments are required to fully align the data set with other Information Standards as specified in the Data Dictionary and to make it fit for use to communicate information between systems i.e. for interoperability. The data set specification is also published on the ISB website.
A minimum required Data Set for each audit have been agreed. These are subsets of the Cataract National Data Set and the AMD National Dataset respectively.

National Cataract Audit

Between 2014 and September 2019, Health Quality Improvement Partnership (HQIP) commissioned the RCOphth to run the first National Ophthalmology Database Audit following a competitive tender in 2013. The project started on 1 September 2014 as a National Cataract Audit (England and Wales) and feasibility studies for audits on glaucoma, Retinal Detachment (RD) and wet Age-related Macular Degeneration (AMD). Since August 2019 the RCOphth has run the NOD independently from HQIP and is open to NHS and private providers of Cataract surgery from the UK and the Channel Islands. It is funded through participation fees from centres as well as donations from industry and charity. Funding organisations are listed on our website https://nodaudit.org.uk/funding.

National Age-related macular degeneration (AMD) Audit
In October 2020, the RCOphth committed to develop a UK national AMD audit following a successful HQIP funded feasibility study. Participation is open to service providers nationally, across the UK and the Channel Islands.

The National AMD Audit collects data to enable providers to compare treatment outcomes for the "wet" or neovascular form of AMD, considering differences in baseline characteristics, to improve compliance, and identify and disseminate best practice to improve key clinical care processes.

The audit provides real-world benchmarks and enables patients, providers and commissioners to compare clinical outcomes and key processes at different sites, to enable informed decision-making and patient choice, and highlight best practice, with the aim to vastly reduce variation in the outcomes of treatment for wet AMD.

1. 3 Legal and regulatory context

The NOD audits are covered under GDPR by the following legal bases for processing data:

- 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 6 (1) (e)}
- 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. {Article 9 (2) (i)}

Information collected is available to a very small number of specially restricted staff on the audit team. The data analyst uses a secure dedicated computer to analyse the information. The College and its subcontractors undertake analysis of the data for the purposes of the audit. However, anonymized and / or aggregated information may be requested for research, service evaluation and commissioning purposes, and information will only be released following approval from the data controller. The Royal College of Ophthalmologists is the data controller and has overall authority over the data and all aspects of its use.

The NOD operates within the UK GDPR key data protection principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

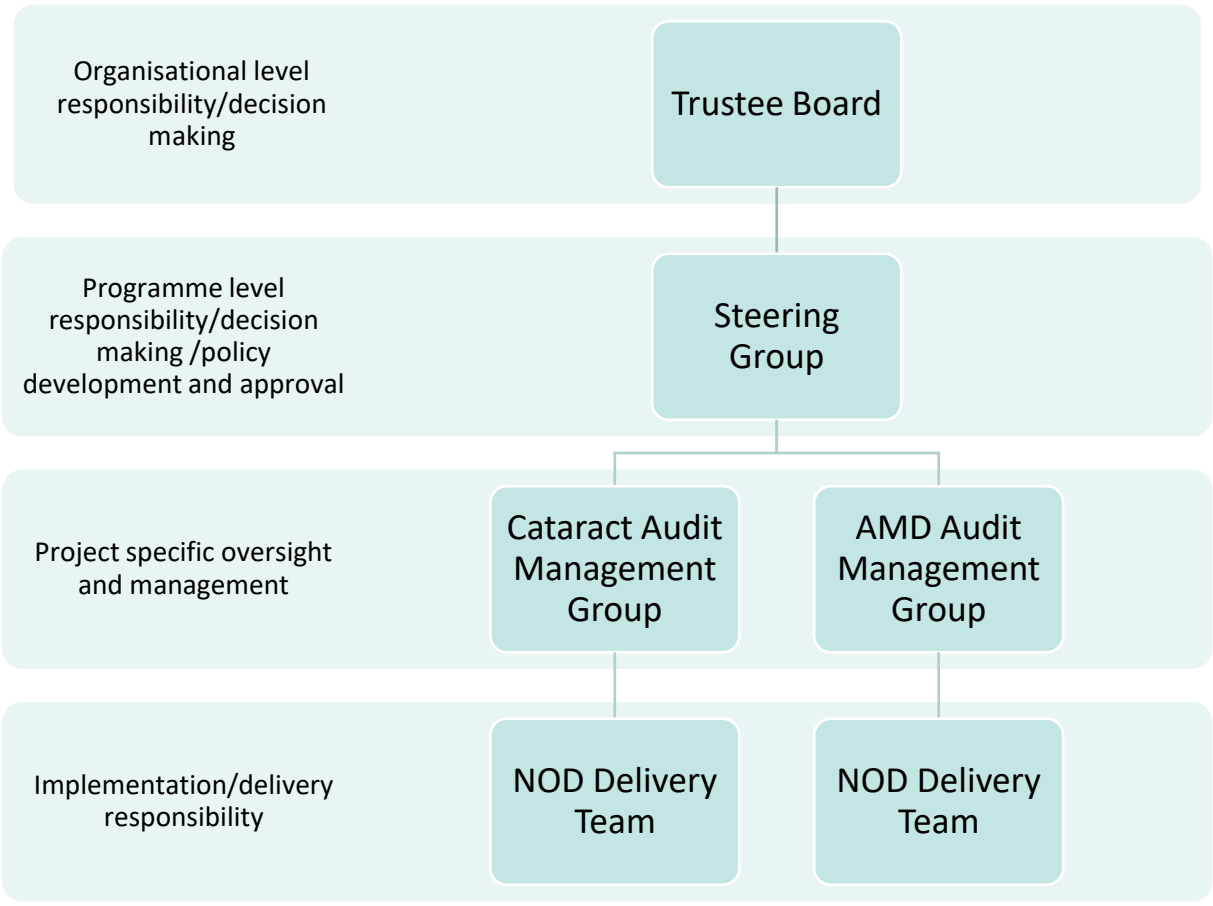
2. Responsibilities

A Steering Group has been set up to oversee the NOD. The Steering Group reports to the Trustee Board. Membership of the Steering Group includes stakeholder organisations and patient representation.

The NOD works with several subcontractors including the original NOD delivery unit based at Cheltenham General Hospital within Gloucestershire Hospitals NHS Foundation Trust (GHNHSFT), EMR subcontractors and IT subcontractors.
Regular performance review meetings are held to ensure progress towards and achievement of deliverables.

There is no industry representation in any of the groups outlined in the structure below. The RCOphth retains independence deciding the data analyses to be performed and reported. All outputs from the analyses are be placed in the public domain.

2.1 NOD Operational Structure



2.2 Data Controller

https://www.nodaudit.org.uk Following on from HQIP commissioning of the National Audit the Data Controller function transferred to HQIP. The RCOphth retains the role of Data Controller for all data prior to the HQIP commissioned audit 'legacy data' collection. The Data

Controller has authority over the data and all aspects of its use, including the release of data for other purposes and is responsible for assuring appropriate use of the data.

Organisations that participated in the NOD during the HQIP commissioned period opted in to the RCOphth retaining their raw data in the NOD. If no positive opt in confirmation was received by the RCOphth, the data was deleted by 30 November 2019 when the honorary contract with HQIP ceased. Data collected and analysed (i.e. not the raw data) during the HQIP commissioned period has been transferred from HQIP to the RCOphth via a data transfer agreement.

RCOphth was the data Controller 2010-September 2014.

Prior to receipt of HQIP funding, the RCOphth was the Data Controller. The work on data from this earlier phase is now complete and published.

Fresh data requests are considered subject to feasibility and availability of the requested data, and subject to relevant IG requirements.

- 2010 Medisoft data extraction performed in 2011 and backdated to 2010 as this was linked to dates of approvals for extraction. (Raw data now deleted)
- October 2013 and August 2014 data received from the BEAVRS RD online audit tool; the August 2014 data was an update of the October 2013 data. (Raw data now deleted)
- October 2013 and December 2014 data were received from VITREOR, the December 2014 data was an update of the October 2013 data. (Raw data now deleted)

HQIP was the Data Controller (September 2014-November 2019).

Data collected as part of work funded by HQIP, including the 'legacy' or historic data extract and the prospective data extracts, were under HQIP IG control until 30 November 2019. The 2015 data extraction was the "first HQIP" set of data and the 2018 data extraction was the last. These data include those for the main cataract audit as well as the feasibility studies on Glaucoma, RD and AMD. Included, for example, are comorbidity and other relevant risk factor data for case mix adjustment of cataract outcomes and pachymetry data relevant to glaucoma.

RCOphth is the Data Controller for data received after November 2019.

2.3 Data Processors

The Data Processors noted here are in addition to the local trust / provider who are responsible for the management of their own Personable Identifiable Data (PID).
The Data Processors are:

1. Medisoft Limited: EMR supplier engaged to extract EMR data from participating centres using EMR systems.
2. Gloucestershire Hospitals NHS Foundation Trust: supplier contracted to process and analyse the data provided to the NOD. All personnel responsible for transferring the data and initial data analysis are covered under Trust Information Security policies and/or specific contracts making express provision for the responsibilities of Data Processors.

3. The Royal College of Ophthalmologists processing the data received via the RCOphth website in accordance with this Information Governance Policy.
4. Specific data sharing projects will be possible via the RCOphth Data Access Request mechanism, which allows for data access by other interested parties.

3. Data collection

3.1 Procedures for collecting the data

Where providers have an existing EMR compliant with nationally agreed datasets, data is extracted from the system where feasible see data flow diagrams (appendix 1).
For organisations with paper-based records, the National Cataract Audit can provide an alternative mechanism for electronic data submission. The National AMD audit is not open to providers with paper-based records.

The NOD system performs the following functions and provides the following services:

1. Allows for electronic upload of deidentified processed ophthalmology episode data from submitting organisations into a secure virtual server. Further details can be found in section 5
2. Acts as a database of stored data from supplying data collection systems
3. Data export capability to allow for data querying and secondary data uses
4. User registration and logon services
5. Web service and query engine capable of presenting analysis of the data to individual surgeons and centres
6. Presentation of selected validated reports to the public.

Data transfer

1. Medisoft or Medisight: Data collected on the Medisoft EMR systems are extracted from each Hospital Eye Services EMR server by the EMR system supplier and transferred via Health and Social Care Network (HSCN) network to a secure FTP server at GHNHSFT.
2. OpenEyes and other EMRS: Data from centres using other EMR systems is extracted by staff within the centre using an in-built NOD compliant data extraction mechanism. Data from one centre transferred via the HSCN network to the secure FTP server within GHNHSFT, while all other centres using other EMR systems transfer their data via the NOD website (www.nodaudit.org/uk).
3. Data from in-house databases is transferred via the NOD website.

Data files uploaded to the NOD website:

- are downloaded by the NOD statisticians for saving on the server at GHNHSFT
- must be password protected by the user with the password provided only to the NOD statistician at GHNHSFT via a separate phone call or text message.
- Files are deleted from the NOD website once downloaded onto the server at GHNHSFT. All data will be stored on a secure server at GHNHSFT, which the NOD statistical analysis team will analyse to produce reports. No patient identifiable data will be visible or derivable from any report.

3.2 Data quality standards

The NOD primarily collates Hospital Eye Services electronically collected data compliant with nationally agreed datasets. These datasets are the minimum data required to achieve the aims of the NOD.

The database currently contains deidentified patients' eye care and general health details and relevant demographics, with limited data for other relevant eye conditions, primarily retinal detachment, glaucoma and age-related macular degeneration. If the project is successful in a future Section 251 exemption https://www.rcophth.ac.uk/standards-publications-research/clinical-data-sets/). the following patient identifiable data will be extracted from the EMR systems and databases of participating centres:

- NHS Number
- Date of birth
- Person Gender Current (Sex)
- Ethnic category (where available)
- Post Code of Usual Address

The NOD does receive data for the person's gender and ethnic category but with the patient deidentified these data items are insufficient to directly identify a patient. For organisations using an EMR the date of birth is randomly perturbed during data extraction (date of birth ± a random number of days between -190 and +190). For organisations using in-house databases they have the option of applying similar date perturbation or supplying the patients age at cataract surgery or age starting "wet" AMD treatment instead of the date or birth.

The RCOphth NOD website is hosted on a secure server with an interfacing capability to allow for data to be received electronically from Hospital Eye Services across the UK.

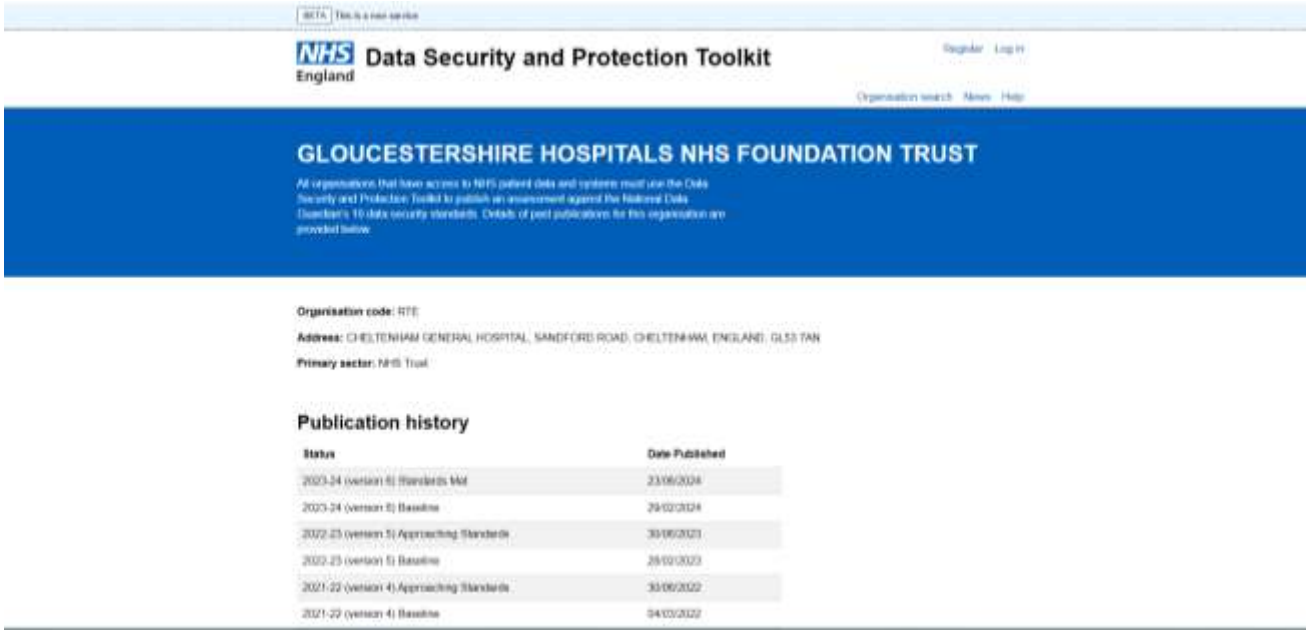
4. Data storage and security

4.1 Storage of clinical data

The NOD database consists of a database hosted on a secure server at GHNHFT. Interfacing standards are open and available for any supplier of EMR systems to adopt. Establishment of the system and the processes for assuring IG processes has been undertaken in consultation with the GHNHSFT IG officers and The Royal College of Ophthalmologists.

Data exported to the NOD statistical support officers is stored on a secure server hosted by GHNHSFT.

GHNHSFT Data Security and Protection Toolkit (DSPT) information: organisation code is RTE. Accessed 9 July 2024 https://www.dsptoolkit.nhs.uk/OrganisationSearch/RTE Standards Met 23/06/2024.



4.2 Analysed data for dissemination

Data reports are presented on the NOD website hosted by Pantheon Systems, Inc. and its affiliates, including Pantheon UK Private Limited, (collectively, "Pantheon") using Google Cloud data centres.

The hosting provider has SOC 2 Type 2 compliance covers the Security and Availability Trust Services Criteria.

Pantheon complies with privacy regulations pursuant to the General Data Protection Regulation (Regulation 2016/769 or GDPR). For the United Kingdom, Pantheon complies with the GDPR and the Data Protection Act of 2018.

5. Encryption and data protection

5.1 Deidentification

The NOD does not hold any patient identifiable data. For organisations using an EMR system. The link to patient identifiers must be destroyed during the extraction and before the related data are transferred to the NOD; therefore, no re-identification of patients is possible. The NOD does not currently have exemption under Section 251 of the NHS Act 2006 ("S251 exemption") and no patient identifiable data will or can be submitted to the NOD.

However, the RCOphth intends to apply for an exemption to facilitate linkage with databases such as those where NHS England is a Data Controller. If S251 exemption is obtained, all centres will be informed of the changed status of the NOD, and permission for data submission/extraction will be revised accordingly.

The data extracted from contributing centres includes the patient gender, ethnicity and a randomly perturbed date of birth (± a random number of days between -190 and +190) but does not include postcode, NHS number or hospital number. The deidentification of all patient identifiable data submitted to the NOD is achieved through the application of a unique

identifier to each patient's data before the data is transferred from a contributing centre to the NOD, at the time of data extraction. The relationship between the NOD identifier and the patient identifiers on the centre's EMR system is not recorded within the submitting EMR system and are not visible to clinicians at those centres. This approach is akin to full anonymisation, because only the source centres and the EMR providers (both of which have access to all the identifiable data, with appropriate governance controls in place) can re-identify patients, regardless of any data linkage that is applied downstream within the same data source. Therefore, no identifiers leave the Trust and the code can link records within the NOD but cannot support linkage to any external dataset.

Non-EMR centres are required to apply the relevant approaches to the deidentification of the data they submit so that no patient identifiable data is transferred to the NOD except for the patient gender, ethnicity and either perturbed date of birth or the patient's age at cataract surgery.

The data once sent to and stored within the NOD therefore contains a unique identifier that **cannot be de-referenced by any Data Processor to identify a patient** but can be used to match new data extractions with the appropriate patient in the future.

The data do include the ability to identify clinicians, although the extent to which clinician data is exposed to viewers of the audit is controlled as described below.

5.2. Access Controls

The server on which submitted data is stored can only be accessed by the NOD team in GHNHSFT and the data is stored on a restricted access sever that only the NOD statisticians can access, with the submitted data stored on separate disc space to all other files. No raw data are or will be stored on any other system (other than the source data collection systems, which in the case of EMR systems are regulated by contract between the EMR provider and each contributing Hospital Eye Service) except where the release of data is approved through the data release process.

Analysed data is available to contributors and the RCOphth staff project team via the NOD website. This comprises an open access section and an access-controlled section with a secure log on.

The public section displays results from analysis of the prospective audits annual data collections.

For the cataract audit this commenced in September 2015 as part of the HQIP commissioned project). Outputs of non-trainee surgeons (National Cataract Audit only) and centres are publicly available on the NOD website.

For display of the legacy data (from the start of 1 April 2010 to the end of March 2015) from the first NOD extract, access controls have been developed to secure access to the results on the contributors' section of the NOD website. Clinicians will only be able to identify their own results or their centre's result in any analysis and will not be able to identify any other centre or individual on these presentations. The system will maintain a user database to authenticate

users' access. The access control module (Log on to the website) was developed in accordance with best practice for IT applications using username and password authentication.

For the AMD audit outputs at centre level are expected to be publicly available on the NOD website in 2025.

6. Data Breach and Information Risk Management

In the event of a data breach or an information security incident, appropriate actions will be taken to minimise associated risks. The approach for managing risks includes a methodical process by which the project team identifies, scores, and ranks the various risks. Every effort is made to proactively identify information risks ahead of time to implement a mitigation strategy.

If a data breach is suspected (within 48 working hours):

1. An investigation will be carried out by the NOD delivery team and reported to the RCOphth Data Protection Officer (DPO)[*] to consider the sensitivity of the data involved.
2. A risk assessment will be performed as to what might be the consequences of the incident, for instance whether harm could come to individuals or whether data access could be unavailable.
3. The RCOphth DPO will advise of any need to contact the Information Commissioners Office based on the extent of the breach.

If a data breach is identified following the investigation:

1. Data breach by RCOphth (within 48 working hours of investigation confirmation)
    a. Incident and actions recorded asap on NOD data breach log
    b. Data deleted and recorded in data breach log
    c. Breach is reported to organisation responsible – data submitted and DPO/Caldicott Guardian/Information Governance
    d. RCOphth DPO notified and review data breach log to confirm appropriate action
2. Data breach by Data processors (within 48 working hours of investigation confirmation)
    a. Incident and actions recorded asap on NOD data breach log
    b. Data deleted and recorded in data breach log
    c. Breach is reported to organisation responsible – data submitted and DPO/Caldicott Guardian/Information Governance
    d. RCOphth DPO notified and review data breach log to confirm appropriate action
3. Data breach by Data Controller submitting PID in data submission directly from the organisation (within 72 working hours of investigation confirmation)
    a. Incident and actions recorded asap on NOD data breach log

[*] Or Chief Executive if the DPO is unavailable

b. Data deleted and recorded in data breach log
c. Breach is reported to organisation responsible – data submitted and DPO/Caldicott Guardian/Information Governance
d. RCOphth DPO notified and review data breach log to confirm appropriate action.

7. Reporting Intent

The audit reports are available on www.nodaudit.org.uk and www.rcophth.ac.uk websites. These audit reports are publicly accessible. The first report was based on historic or 'legacy' data and provided a mechanism for refinement of the methodology. Information included in the initial report is limited as the audit was in a developmental phase.

7.1 National Cataract Audit

All named surgeon and centre outputs are publicly available on www.nodaudit.org.uk website. This includes case complexity adjusted outcomes for Posterior Capsular Rupture (PCR) and Visual Acuity (VA) Loss from cataract surgery for named consultant and independent surgeons, and for named surgical centres. For prospective audit data from 31 August 2019 these data will continue to be published on the NOD website.

7.2 National AMD Audit

The NOD will not publish or report information that will identify individual members of staff. All centre level outputs will be publicly available, when there is sufficient confidence in the data quality, on www.nodaudit.org.uk. This may include (subject to data quality):

- Percentage of eyes for which treatment was offered or started (when appropriate) within 14 days of referral
- Percentage of eyes completing the loading phase of 3 injections, within 10 weeks of the first injection
- Percentage of visits for which follow-up was delayed by more than 14 days after planned interval on at least one occasion in the first 12 months
- Median visual acuity changes from baseline to months 12 and 24
- Percentage of eyes with visual acuity ≥70 letters (almost driving standard) at the start of treatment
- Percentage of eyes with follow up data up to one year of treatment
- Percentage of eyes with visual acuity data at both the start of treatment and after one year of treatment
- Percentage of eyes with visual acuity ≥70 letters (almost driving standard) after 12 and 24 months
- Percentage of eyes losing ≥10 letters of visual acuity at one year of treatment

If processed data is requested from the NOD by legitimate bodies such as the Care Quality Commission (CQC), Getting It Right First Time (GIRFT) and data.gov.uk, such requests will be accommodated where feasible.

8. Resolving local Information Governance Concerns

The RCOphth has provided information in the form of a letter to help Clinical Directors / Leads and Caldicott Guardians (or equivalent) make the decision to become a contributing centre. Individual organisations are invited to confirm in writing that data from their institution may be extracted and included in the audit. Prior to the data extraction, this letter was distributed to all Caldicott Guardians or Guardian equivalent and Clinical leads as part of the request for them to participate in the audit. Only once agreement is received from both the Caldicott Guardian or Guardian equivalent and the Clinical Lead, will a data extraction be undertaken.

9. Releasing data to third parties

9.1 Access to NOD data for research or audit purposes

Applicants who wish to use data held on the NOD for research or audit purposes must complete and submit the data sharing agreement form and the data access request form to the NOD via noa.project@rcophth.ac.uk.

Not all enquiries progress to the application stage, for example:

- If the information requested is available through existing published data.
- If the NOD does not contain the data required.
- If data from a specific extraction has been deleted by the NOD according to the data retention timelines (see section 10).

Data from these projects is routinely reported and these reports are available on the NOD website.

If a data access application is necessary, applicants are advised to contact the RCOphth before applying. This will allow us to inform you that the data requirements can be met and review your application ahead of it being submitted for consideration.

9.1.2 When we can release data

We can only authorise the release of data for which the RCOphth is the data controller. Some data we collect is not placed in the public domain. However, as the data controller, we can share this data for the purpose of quality improvement, including research, service evaluation, and audit, if certain conditions are met and depending upon permissions in place for each project.

The RCOphth cannot usually give permission to share data for which we are not a data controller; this includes projects involving linkage to a dataset controlled by another organisation. It is important that when you would like to access a linked dataset, you discuss this with the RCOphth before an application is submitted.

9.1.3 Outputs or reports

The RCOphth is committed to ensuring that, where possible, all data, outputs and publications are made publicly available for the benefit of the public and the NHS.

Applicants, especially for the purposes of research, are expected to publish any findings or outputs resulting from their analysis of NOD data. Applicants should reference that the data used was collected by the NOD. The acknowledgement should take this form:
Data has been provided by The Royal College of Ophthalmologists National Ophthalmology Database audit from the xxx Programme

To be transparent, the RCOphth will publish a public register of approved data sharing applications.

10. Data Retention

Each data extract received is retained for 5 years, and then deleted at the end of this 5-year period provided analyses have been fully completed and published. The data extract includes raw data at patient level. Processed data is reported for the relevant analysis period for specific analyses, which may be longer than 5 years. The NOD only retained data submitted during the period it was commissioned by HQIP if the contributing organisation signed an opt in agreement for retention of data.

Data which have been approved through the data sharing process could remain with the provider in line with the data sharing agreement.

Yearly data extraction: Participating centres can use the annual data submission as an opportunity to re-extract and re-submit data from previous audit years. No single data extract is retained for longer than 5 years.

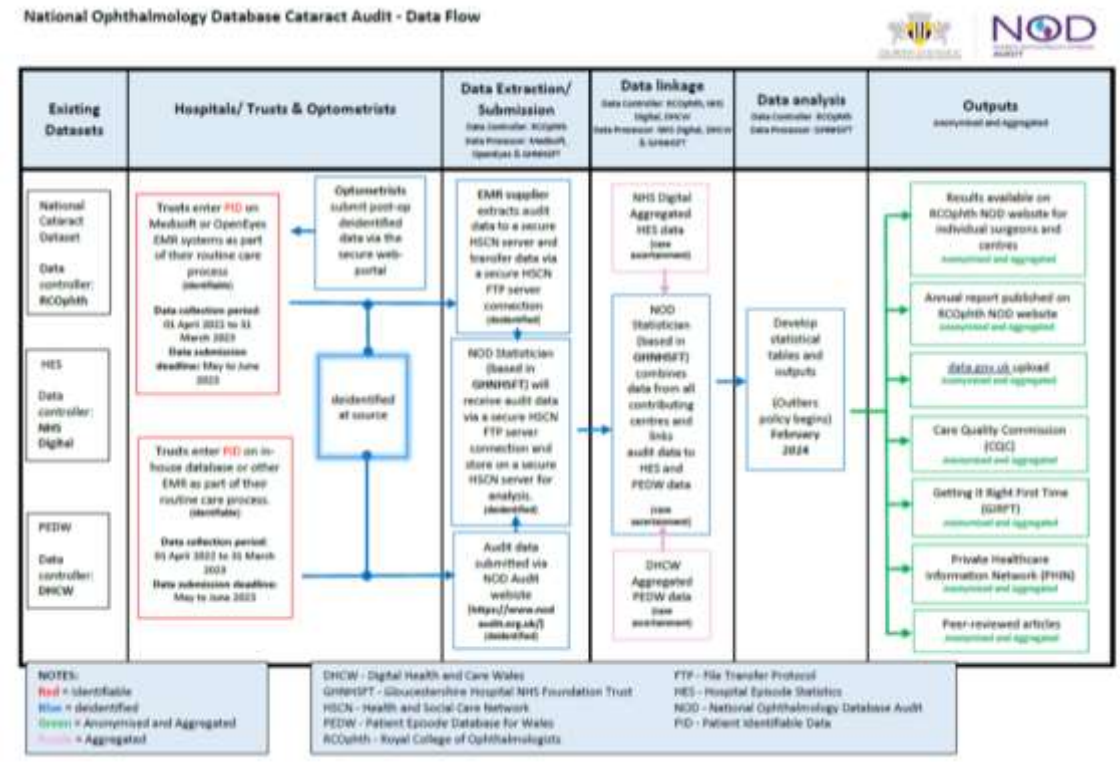
Advantages of re-submitting historical data include:

1. If there have been any amendments to data we have previously received, the re-extracted data will contain these. This has benefitted many surgeons who have found errors or data not recorded that has negatively influenced their results. We make any agreed changes to the results, and we ask them to update the data on their local system, in conjunction with their local clinical lead or relevant person who has the necessary access rights and IG authority to make retrospective corrections to patient records. The next data extraction then contains the corrected data.
2. We can receive missing follow up data for patients treated in previous extractions who had not had their follow up data recorded in time for the earlier extraction e.g. for patients who have surgery in the latter months of an audit year would not always have the postoperative follow up information recorded by the time of data extraction. By re-extracting the data from the previous audit year, we can receive any follow up data that was recorded after the previous data extraction. This helps with the completeness and overall accuracy of post-surgery results.

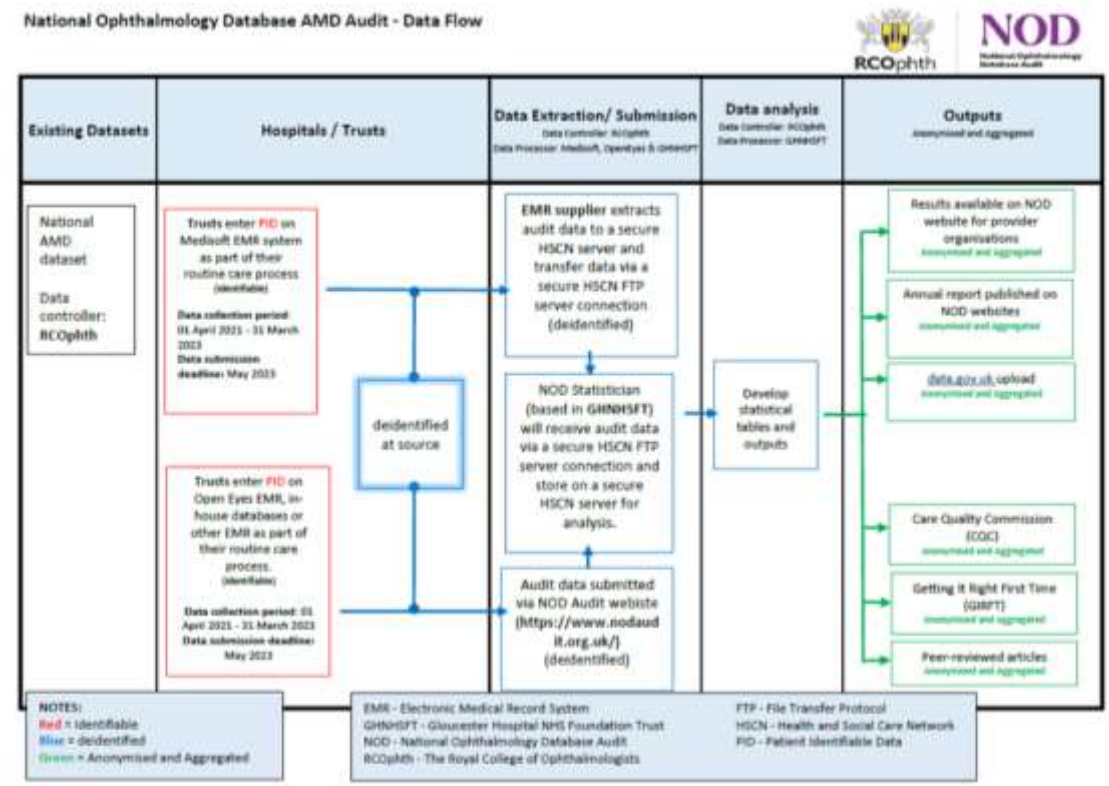
On completion of the audit contract, processed summary data is uploaded onto data.gov.uk at the same granularity of the report.

Appendix 1 Data Flow Diagrams

National Cataract Audit data flow



National AMD Audit data flow



Appendix 2 List of abbreviations found in this document

AMD	Age-Related Macular Degeneration
CQC	Care Quality Commission
DSA	Data Sharing Agreement
DSPT	Data Security and Protection Toolkit
EMR	Electronic Medical Record
GDPR	General Data Protection Regulation
GHNHSFT	Gloucestershire Hospitals NHS Foundation Trust
HSCN	Health and Social Care Network
HQIP	Healthcare Quality Improvement Partnership
IG	Information Governance
ISB	Information Standards Board
ISO	International Organization for Standardisation
GIRFT	Getting It Right First Time
NHS	National Health Service
NOD	National Ophthalmology Database
PCR	Posterior Capsular Rupture
PID	Personable Identifiable Data
RCOphth	The Royal College of Ophthalmologists
RD	Retinal Detachment
SIRO	Senior Information Risk Owner
UK	United Kingdom
VA Loss	Visual Acuity Loss