Policy Document

National Ophthalmology Database Audit: Information Governance Overview V1.6

Date of issue	14 January 2020
Review date	January 2022
Approved by	Informatics and Audit Sub-committee
Document Owner	The Royal College of Ophthalmologists

Contents

List of abbreviations found in this document

AMD	Age-Related Macular Degeneration
CQC	Care Quality Commission
DARG	Data Access Request Group
EMR	Electronic Medical Record
GHNHSFT	Gloucestershire Hospitals NHS Foundation Trust
HQIP	Healthcare Quality Improvement Partnership
IG	Information Governance
ISB	Information Standards Board
ISO	International Organization for Standardisation
NCAPOP	National Clinical Audit and Patient Outcomes Programme
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

1 Introduction

1.1 Purpose of Paper

This paper has been produced to outline the Information Governance (IG) issues that impact on The Royal College of Ophthalmologists' (RCOphth) National Ophthalmology Database (NOD) Audit project and to explain how these are managed. It is intended that this document will be of use to Caldicott Guardians, Senior Information Risk Owner (SIRO) and Information Governance Officers when deciding whether to participate in the RCOphth NOD project. The document is also intended to demonstrate that the RCOphth NOD project has been developed in accordance with best practice with regards to Information Governance and is transparent on all aspects of IG and complies with statutory IG guidance.

1.2 Background

The RCOphth NOD project was developed under the auspices of The Royal College of Ophthalmologists, which initially acted as the Data Controller. The aims of the RCOphth NOD have been 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. The initial focus was on Diabetic Eye Disease and cataract surgery (although data were collated for all eye diseases that either had nationally agreed datasets or consistently collected structured data even in the absence of nationally agreed datasets). All data were collected as a by-product of routine clinical care using Electronic Medical Records (EMR) systems used in Hospital Eye Services. All United Kingdom (UK) centres that used EMR systems were invited to contribute pseudonymised data (from which individual patients cannot be identified: see section 4 below) and the RCOphth NOD is not limited to any particular EMR or database supplier, having to date included data from 11 separate suppliers. The RCOphth NOD project was initially seed-funded for one year from September 2009 to August 2010 by the Department for Health via the English National Screening Programme for Diabetic Retinopathy to demonstrate feasibility. The next phase of development was to make reports available to users and further expand the audit capabilities of the system and deliver peer reviewed publications. One early objective of the project was to develop a web-based tool that allowed contributing centres and individual clinicians to see their own performance and compare it with that of their anonymised peers around the UK. This was achieved for posterior capsular rupture (PCR), which is the most common operative complication during cataract surgery and has high validity as a marker of surgical skill. In the context of benchmarking, the RCOphth NOD has the potential to be a useful tool for every ophthalmologist in the UK regardless of whether they can contribute data.

HQIP National Ophthalmology Audit

In 2014, the RCOphth was commissioned by the Healthcare Quality Improvement Partnership (HQIP) to run the first National Ophthalmology Database Audit following a competitive tender in 2013. The project officially started on 1 September 2014 and consisted of a National Cataract Audit (England and Wales) and feasibility studies for audits on glaucoma, Retinal Detachment (RD) and wet Age-related Macular Degeneration (AMD). The audit was initially funded for three years from September 2014 to August 2017 and was successfully extended for a further two years from September 2017 to August 2019. The

HQIP commissioned work covered providers of NHS funded cataract surgery in England and Wales.

2   Data collection

Where providers have an existing EMR compliant with nationally agreed datasets, data can be extracted from the system where feasible.

For organisations with paper-based records, the project can provide an alternative mechanism for electronic data submission. The RCOphth 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.

3. Oversight

A National Audit Steering Committee has been set up to oversee the RCOphth NOD. The Steering Committee reports via the RCOphth Council to the Trustee Board. Membership of the committee includes stakeholder organisations and patient representation.

The RCOphth works with several subcontractors including the original RCOphth NOD delivery unit based at Cheltenham General Hospital within Gloucestershire Hospitals NHS Foundation Trust (GHNHSFT), EMR subcontractor and IT subcontractor.

Regular performance review meetings are held with the RCOphth, to ensure progress towards and achievement of deliverables.

4. Physical System security

The RCOphth NOD database consists of a database hosted on a secure server. 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 RCOphth NOD statistical support officers is stored on a secure server hosted by GHNHSFT. This server can only be accessed by the RCOphth NOD team in

GHNHSFT and the data is stored in a restricted access folder that only the RCOphth NOD statisticians can access. 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 RCOphth data release process.

GHNHSFT Data Security and Protection Toolkit (DSPT) information: organisation code is RTE.

Accessed 16 December 2019

Data held on the RCOphth NOD website is managed by Hypergram and hosted by Nimbus Hosting Ltd which uses VIRTUS Data Centres LTD. data centre in London. The hosting provider complies with current International Organisation for Standardisation standards (ISO27001:2013) for Data Centre management. ISO27001 covers the management activities and physical security standards for maintaining and provisioning services in data centres. As such it provides a level of guarantees in relation to hosted services and provides the RCOphth NOD project with a high level of confidence in relation to physical data security. See appendix 1.

The RCOphth NOD primarily collates Hospital Eye Services electronically collected data compliant with nationally agreed datasets (e.g. the cataract national dataset https://www.rcophth.ac.uk/standards-publications-research/clinical-data-sets/).   These datasets are the minimum data considered necessary to achieve the aims of the National Clinical Audit and Patient Outcomes Programme (NCAPOP) audit. The database currently contains deidentified patients' eye care and general health details and relevant demographics for cataract surgery, 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 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 RCOphth 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 instead of the date or birth.

Data are extracted from each Hospital Eye Services EMR server by the EMR system supplier and transferred via N3 network to a secure FTP server at GHNHSFT. Data from in-house databases can be transferred via the RCOphth NOD website and downloaded and deleted by the RCOphth NOD statistician based at GHNHSFT. Data files uploaded to the RCOphth NOD website must be password protected by the user and the password will be made know via a separate phone call with the RCOphth NOD statistician. Files will be deleted from the RCOphth NOD website once downloaded onto the N3 server at GHNHSFT. All data will be stored on a secure server at GHNHSFT which the RCOphth NOD statistician will analyse to produce reports. No patient identifiable data will be visible or derivable from any report.

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.

Prior to HQIP funding and NCAPOP inclusion the RCOphth was the official Data Controller (as defined in the Data Protection Act 1998) for the RCOphth NOD system. Following on from HQIP commissioning of the National Audit the Data Controller function was 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 RCOphth NOD during the HQIP commissioned period were asked to opt in to the RCOphth retaining their raw data in the RCOphth NOD. If no positive opt in confirmation has been received by the RCOphth, the data was deleted by 30 November 2019 when the honorary contract with HQIP ceased. Data collected and analysed (e.g. not the raw data) during the HQIP commissioned period has been transferred from HQIP to the RCOphth via a data transfer agreement.

The Data Processors are (i) EMR supplier engaged to extract EMR data from participating centres using EMR systems and (ii) Gloucestershire Hospitals NHS Foundation Trust. 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. Specific data sharing projects will be possible via the RCOphth Data Access Request mechanism which allows for data access by other interested parties. The Data Processors noted here are in addition to the local trust / provider who are responsible for the management of their own PID.

5. Deidentification

The RCOphth NOD does not and will not hold any patient identifiable data. For organisations using an EMR system, the link to patient identifiers must be destroyed by the EMR supplier before the related data are transferred to the RCOphth NOD and added to the Database; therefore, no re-identification of patients is possible. The RCOphth 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 RCOphth NOD. However, the RCOphth intends to apply for an exemption to facilitate linkage with our databases such as those that NHS Digital is a Data Controller. If S251 exemption is obtained then all centres will be informed of the changed status of the RCOphth 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 RCOphth NOD will be achieved through the application of a unique identifier to each patient's data before the data is transferred from a contributing centre to the RCOphth NOD, at the time of data extraction. The relationship between the RCOphth NOD identifier and the patient identifiers on the centre's EMR system will not be 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 can be applied downstream within the same data source. Therefore, no identifiers leave the Trust and the code can link records within the RCOphth 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 RCOphth 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 RCOphth 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.

6. Audit Data Sets

The data sets for the RCOphth NOD Audit can be accessed via the RCOphth NOD Audit website, https://www.nodaudit.org.uk/resources/guides.

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, a subset of the Cataract National Data Set, has been agreed for the RCOphth NOD Audit.

7. Access Controls

The RCOphth NOD Audit website comprises an open access section and an access-controlled contributors section with a secure log on.

The public section will display results from analysis of the prospective cataract audits (annual data collections commenced in September 2015 as part of the HQIP commissioned project). Outputs of non-trainee surgeons and centres are publicly available on the RCOphth NOD website.

For display of the legacy data (from the start of 1 April 2010 to the end of March 2015) from the first RCOphth NOD extract, access controls have been developed to secure access to the results on the contributors' section of the RCOphth NOD web site. 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 in order to authenticate users' access. The access control module (Log on to the website) has been developed in accordance with best practice for IT applications using username and password authentication.

8. 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 for the RCOphth NOD Project includes a methodical process by which the project team identifies, scores, and ranks the various risks. Every effort will be made to proactively identify information risks ahead of time to implement a mitigation strategy.

Procedures are in place to ensure that all data breaches are logged and reported to the Trustee Board immediately when they are identified. An investigation will be carried out to consider the sensitivity of the data involved and 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.

If a breach involving personal data has occurred, the Trustee Board will be notified and the RCOphth will inform the Information Commissioner's Office within 72 hours if necessary, based on the extent of the breach.

9. Reporting Intent

The audit reports for all contributing centres 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 it provided us with a mechanism for refinement of the methodology. Information included in the initial report is limited as the audit was in a developmental phase.

For the first prospective annual report and for future audit reports, named surgeon and centre outputs are publicly available on www.nodaudit.org.uk website and also on My NHS (https://www.nhs.uk/service-search/Performance/Search) website as part of the Clinical Outcomes Publication. This will include case complexity adjusted outcomes for PCR and visual acuity 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 RCOphth NOD website.

If processed data is requested from the RCOphth NOD by legitimate bodies such as CQC, GIRFT and data.gov.uk, such requests will be accommodated where feasible.

10. Resolving local Information Governance Concerns

The RCOphth NOD has provided information in the form of a letter that will help Clinical Directors / Leads and Caldicott Guardians to 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 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 and the Clinical Lead, will a data extraction be undertaken.

11. Use of the RCOphth NOD System for Research Purposes

The RCOphth is the Data Controller for all current data.

11.1 Data for which RCOphth is data controller 2010 to date

Prior to receipt of HQIP funding the RCOphth was the Data Controller for the RCOphth NOD project. The work on data from this earlier phase of the RCOphth NOD is now complete and published. Fresh data requests will be considered subject to feasibility and availability of the requested data, and subject to relevant IG requirements.

- 2010 Medisoft data extraction performed in 2011 and back dated to 2010 as this was linked to dates of approvals for extraction.
- 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.
- October 2013 and December 2014 data were received from VITREOR, the December 2014 data was an update of the October 2013 data.

- Data received after 31 August 2019.

11.2 Data for which HQIP was the Data Controller (2014-2019)

Under HQIP regulations HQIP was the data controller for data collected as part of all work funded by them which means that 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 which are relevant to glaucoma.

11.3 Access to RCOphth NOD data for research or audit purposes

Applicants who wish to use data held on the RCOphth NOD for research or audit purposes must complete and submit the RCOphth data sharing agreement form and the data access request form to the RCOphth at 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. Please read the following information to see if the data you require is available from another source before proceeding with your application.
- If the RCOphth NOD does not contain the data you require.

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

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

11.3.1 When we can release data

We can only authorise the release of data for which the RCOphth NOD is the data controller.

Some data that 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 NOD 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, such as NHS Digital. It is important that when you would like to access a linked dataset, you discuss this with the RCOphth NOD team before an application is submitted.

11.3.2 Submitting an application

If the RCOphth NOD team has advised an application would be appropriate, complete the data access request form as required. Download the form from the RCOphth NOD website. Applications are reviewed on a monthly basis.

Completion of all relevant sections of the application form is needed along with providing all relevant supporting information and signatures of the applicants.

The application form has embedded terms and conditions and together they form the data sharing agreement (DSA). All applicants and the data provider are required to sign this document before we authorise the release of data to you.

11.3.3 What happens to applications after submission?

The RCOphth NOD will confirm receipt of the request and undertake an initial review of each application within 6 weeks of submission.

After the initial review, your application will be referred to the RCOphth Chair of Professional Standards, Chief Executive and President or, if the application has not been satisfactorily completed, it will be returned for clarification or seeking further information.

Each application is reviewed against the following criteria:

- Does the RCOphth NOD hold the requested data?
- Is the proposed use of the data clinically appropriate?
- Is the proposed use of the data methodologically sound?
- Does the application satisfy the requirements of the GDPR and Data Protection Act 2018?
- Are the necessary legal and ethical permissions and security arrangements in place?

We will inform applicants of the outcome of a meeting within ten working days of the meeting.

Following approval, data will be released within a reasonable timeframe agreed with the data processor. This may vary depending upon the complexity of the date requested and the scope of the core audit activity being undertaken at that time. Discussion of any deadlines or timescales can be done before applying.

11.3.4 Outputs or reports

The RCOphth and the NOD are 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 for data, especially for the purposes of research, are expected to publish any findings or outputs resulting from their analysis of RCOphth NOD data. Applicants should reference that the data used was collected by the RCOphth NOD. The acknowledgement should take this form:

Data has been provided by The Royal College of Ophthalmologists National Ophthalmology audit Database from the xxx Programme

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

12. Data Retention

Each data extract received by the RCOphth NOD will be 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 will be reported for the relevant analysis period for specific analyses, which may be longer than 5 years.

Yearly data extraction: Participating RCOphth NOD centres can use the annual data submission as an opportunity to re-extract and re-submit data from previous audit years. There are advantages to re-extracting data each year and this is automatic for centres using the Medisoft EMR, but as noted above, no single data extract will be retained for longer than 5 years.

Advantages of yearly data extractions 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 at our end and we ask them to update the data on their local system, which many have done 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 had surgery in August 2017, for whom the RCOphth NOD received the data in November 2017, many records would not yet have the postoperative follow up information recorded. By re-extracting data in November 2018, we receive any follow up data from November 2017 onwards, which helps with the completeness and overall accuracy of post-surgery results.

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

- The audit will retain HQIP data until the end of the contract. Beyond the HQIP commissioned audit period data for which HQIP is the data controller will only be retained if the contributing organisation has signed an opt in agreement for retention of data.

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

Certificate GB12/85531

SGS

The management system of

Coreix

Refuge House, 9-10 River Front, Enfield, London, EN1 3SZ, UK

Unit 3, Trade City, Crown Road, Enfield, EN1 1TX, UK

has been assessed and certified as meeting the requirements of

ISO/IEC 27001:2013

For the following activities

The Information Security Management System supports the protection of sensitive Information for both Coreix and its clients during the provision of High Availability Hosting Solutions and Colocation Services. The management system scope includes all operations within the companies Secure Data Centre and Offices located in Enfield within the following boundaries; Information Technology systems, support and services as well as general business operations including finance, human resources, sales and marketing. In accordance with the companies Statement of Applicability Version 3.

This certificate is valid from 27 April 2015 until 27 April 2018 and remains valid subject to satisfactory surveillance audits. Re certification audit due before 13 April 2018 Issue 2. Certified since 27 April 2012
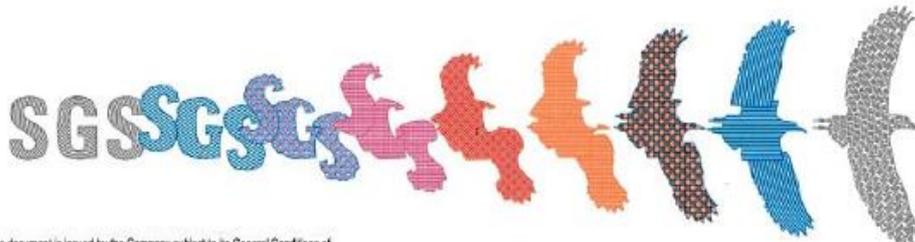
Authorised by

SGS United Kingdom Ltd   Systems & Services Certification
Rossmore Business Park   Ellesmere Port   Cheshire   CH65 3EN   UK
t +44 (0)151 350-6666   f +44 (0)151 350-6600   www.sgs.com

SGS 27001 01 0714

Page 1 of 1

UKAS
MANAGEMENT
SYSTEMS
0005