



---

## Policy Document

# National Ophthalmology Database Audit: Information Governance Overview V1.9

---

18 Stephenson Way, London, NW1 2HD T. 020 7935 0702  
contact@rcophth.ac.uk rcophth.ac.uk @RCOphth

© The Royal College of Ophthalmologists 2018 All rights reserved  
For permission to reproduce any of the content contained herein please contact contact@rcophth.ac.uk

## Contents

---

Section	page
List of abbreviations found in this document	3
1 Introduction	4
1.1 Purpose of Paper	4
1.2 Background	4
1.3 HQIP National Ophthalmology Audit	4
2. Oversight	6
3. Physical System security	6
4. Pseudonymisation	7
5. Audit Data Sets	8
6. Access Controls	8
7. Data Breach and Information Risk Management	9
8. Reporting Intent	9
9. Resolving local Information Governance Concerns	9
10. Use of the NOD System for Research Purposes	10
10.1 Data outside of the scope of the HQIP funded National Ophthalmology Audit for which the RCOphth has been the Data Controller	10
10.2 Data for which HQIP is the Data Controller	10
11. Data Retention	11
Appendix 1 Certificate of compliance with ISO 27001	12

## List of abbreviations found in this document

---

EMR	Electronic Medical Record
GHNHSFT	Gloucestershire Hospitals NHS Foundation Trust
HQIP	Healthcare Quality Improvement Partnership
IG	Information Governance
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
RCOphth	The Royal College of Ophthalmologists
SSL	Secure Sockets Layer
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 NOD project. The document is also intended to demonstrate that the 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 NOD project was developed under the auspices of The Royal College of Ophthalmologists, which initially acted as the Data Controller. The aims of 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 NOD is not limited to any particular EMR or database supplier, having to date included data from 11 separate suppliers.

The 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, NOD has the potential to be a useful tool for every ophthalmologist in the UK regardless of whether they are able to contribute data.

## 1.3 HQIP National Ophthalmology Audit

The Healthcare Quality Improvement Partnership (HQIP) is led by a consortium of the Academy of Medical Royal Colleges, the Royal College of Nursing and National Voices. Its aim is to promote quality improvement in patient outcomes, and in particular, to increase the impact that clinical audit, outcome review programmes and registries have on healthcare

---

quality in England and Wales. HQIP holds the contract to commission, manage and develop the National Clinical Audit and Patient Outcomes Programme (NCAPOP), comprising around 40 projects covering care provided to people with a wide range of medical, surgical and mental health conditions. The programme is funded by NHS England, the Welsh Government and, with some individual projects, other devolved administrations and crown dependencies. [www.hqip.org.uk/national-programmes](http://www.hqip.org.uk/national-programmes). For the purposes of this audit, all centres undertaking NHS funded cataract surgery in England and Wales are expected to contribute data.

The RCOphth was commissioned in 2014 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 consists 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 this has now been extended for a further two years from September 2017 to August 2019. The feasibility studies on glaucoma, retinal detachment and wet age-related macular degeneration have been completed and the audit will now focus on cataract surgery and a feasibility study on the collection of Patient Reported Outcome Measures (PROMs) for cataract surgery in the extension period. The project builds on the existing NOD work and has been extended to cater for all providers of NHS funded cataract surgery in England and Wales.

Where providers have an existing EMR compliant with nationally agreed datasets, data can be extracted from the system where feasible. For NHS Trusts with paper based records, the project will provide an alternative mechanism for electronic data submission. Following a competitive tender process, the College contracted with Medisoft Limited to provide a data collection tool which also includes functionality allowing for post-operative data to be entered by community optometrists.

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

1. Allows for electronic upload of pseudonymised (or PID data subject to a successful Section 251 exemption application) ophthalmology episode data from EMR systems (compliance to interfacing standards required by EMR system) into a secure virtual server. Further details on pseudonymisation can be found in section 4;
2. Acts as a database of stored data from EMR systems;
3. Data export capability to allow for data cleansing 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 after discussions with HQIP.

## 2. Oversight

---

When the NOD was founded the RCOphth acted as the data controller and established a NOD Board which was responsible for the day to day running of the project. Following receipt of HQIP funding and inclusion within National Clinical Audit and Patient Outcomes Programme (NCAPOP) a National Audit Steering Committee was set up to oversee the HQIP funded national audit. The Steering Committee is chaired by the Clinical Lead for the National Audit and reports via the Informatics and Audit Sub-committee to the Professional Standards Committee and ultimately to the College Trustee Board. Membership of the committee is in accordance with HQIP and NCAPOP requirements and includes stakeholder organisations and patient representation.

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

Regular contract review meetings are held with the commissioners, HQIP, to ensure progress towards and achievement of deliverables.

## 3. Physical System security

---

The NOD database consists of a database hosted on a secure server with an interfacing capability to allow for data to be received electronically from EMR systems in Hospital Eye Services across the UK. 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, and conform to HQIP requirements.

Data exported to the NOD statistical support officers is stored on a secure server hosted by GHNHSFT. This server can only be accessed by the NOD team in GHNHSFT and the data is stored in a restricted access folder that only the NOD statisticians can access. No raw data are or will be stored on any other system (other than the source EMR systems, which are regulated by contract between the EMR provider and each contributing Hospital Eye Service) except where the release of data is approved through the HQIP and College data release process. GHNHSFT IG toolkit information: organisation code is RTE, IG toolkit version 14.1 (2017 - 2018), published with a score of 76%.

Data held on the NOD website is managed by Hypergram and hosted by Nimbus Hosting Ltd which uses Coreix data centre in Enfield. The hosting provider complies with current International Organisation for Standardisation standards (ISO27001) 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 NOD project with a high level of confidence in relation to physical data security. [See appendix 1.](#)

NOD primarily collates Hospital Eye Services EMR data based on 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 NCAPOP audit. The database currently contains pseudonymised patients' eye care and general health details and relevant demographics across relevant eye conditions, primarily but not exclusively, cataract, retinal detachment, glaucoma and age-related macular degeneration. If the project is successful in its Section 251 exemption the following patient identifiable data will be extracted from the EMR systems and databases of participating centres in England & Wales:

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

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. Similarly, data from in-house databases will be transferred via a secure website, <https://nww.sft.nhs.uk> (N3 to N3) to the NOD statistician based at GHNHSFT. All data will be stored on a secure server at GHNHSFT which the NOD statistician will analyse to produce reports. No patient identifiable data will be visible or derivable from any report.

Prior to HQIP funding and NCAPOP inclusion the RCOphth was the official Data Controller (as defined in the Data Protection Act 1998) for the NOD system. Following on from HQIP commissioning of the National Audit the Data Controller function has been 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.

The Data Processors are (i) EMR supplier engaged to extract EMR data from participating centres 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 HQIP Data Access Request mechanism which allows for data access by other interested parties.

## 4. Pseudonymisation

---

The data extracted from contributing centres includes a randomly perturbed date of birth ( $\pm$  a random number of days between -190 and +190) but does not include postcode, NHS number or hospital number. The pseudonymisation of all patient identifiable data submitted to NOD will be achieved through the application of a unique identifier to each patient's data transferred from a contributing centre to NOD, at the time of data extraction (i.e. before any data are transferred to the national audit database). The relationship between the NOD identifier and the patient identifiers on the centre's EMR system will only 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 pseudonymisation code can link records within NOD but cannot support linkage to any external dataset.

The data once sent to and stored within 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. Audit Data Sets

---

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

The Royal College of Ophthalmologists 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 NOD Audit.

## 6. Access Controls

---

The NOD Audit website will comprise 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). Outputs of non-trainee surgeons and centres are publicly available on the NOD website.

For display of the legacy data (up 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 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.

## 7. 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 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 HQIP 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, HQIP will be notified and they will inform the Information Commissioner's Office within 72 hours if necessary, based on the extent of the breach.

## 8. Reporting Intent

---

The audit reports will be available on [www.nodaudit.org.uk](http://www.nodaudit.org.uk) and [www.hqip.org.uk](http://www.hqip.org.uk) websites. All audit reports will be 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 will be publicly available on [www.nodaudit.org.uk](http://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 surgical complications and visual acuity loss from cataract surgery for named consultant and independent surgeons, and for named surgical centres.

Summary aggregated data for named centres will be provided to CQC and uploaded on [data.gov.uk](http://data.gov.uk) website at the same granularity of the audit report.

## 9. Resolving local Information Governance Concerns

---

The 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 NHS Trusts 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.

## 10. Use of the NOD System for Research Purposes

---

HQIP is the Data Controller for all current data.

### 10.1 Data outside of the scope of the HQIP funded National Ophthalmology Audit for which the RCOphth has been the Data Controller

Prior to receipt of HQIP funding the RCOphth was the Data Controller for the NOD project. The work on data from this earlier phase of the NOD is now mostly complete and published. Fresh data access requests are no longer being considered for the RCOphth controlled data.

- 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 was received from VITREOR, the December 2014 data was an update of the October 2013 data.

### 10.2 Data for which HQIP is the Data Controller

Under HQIP regulations HQIP is 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 are under HQIP IG control until August 2019. The 2015 data extraction was the "first HQIP" set of data. 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.

Applicants who wish to use data held on NOD for research or audit purposes must complete and submit the HQIP data sharing agreement form and the data access request form to the RCOphth at [noa.project@rcophth.ac.uk](mailto:noa.project@rcophth.ac.uk).

- [HQIP's Data Sharing Agreement](#)
- [HQIP's Data Access Request Form](#)

On receipt of the completed forms, the application will be considered by the RCOphth NOD data release advisory group, who will advise HQIP if the data requested is available on the NOD. The College may request that the application be revised and will then pass on the application to HQIP for review by its Data Access Request Group (DARG).

In relation to secondary uses of data to support research projects contributing centres can be assured that written evidence of ethics committee and research governance approvals, or exemptions therefrom, will be required by any prospective researcher. Data release from the NOD system will be dependent upon receipt of such approvals.

## 11. Data Retention

---

- On completion of the audit contract, processed summary data will be uploaded onto [data.gov.uk](https://data.gov.uk) at the same granularity of the report.
- The audit will retain HQIP data until the end of the contract with HQIP after which data retention will be determined by HQIP.
- Data which have been approved through the HQIP DARG process could remain with the provider in line with the data sharing agreement.

# Appendix 1 Certificate of compliance with ISO 27001

Certificate GB12/85531

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

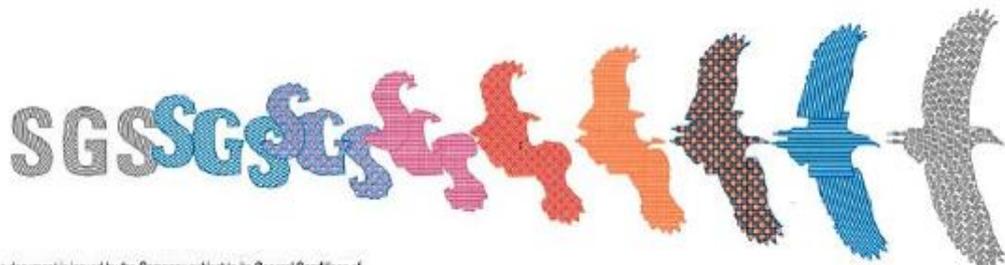
SGS United Kingdom Ltd Systems & Services Certification  
Rossmore Business Park Ellesmere Port Cheshire CH65 3EN UK  
t +44 (0)151 350-6666 f +44 (0)151 350-6600 www.sgs.com

SGS 27001 01 0714

Page 1 of 1



0005



This document is issued by the Company subject to its General Conditions of Certification Services accessible at [www.sgs.com/terms\\_and\\_conditions.htm](http://www.sgs.com/terms_and_conditions.htm). Attention is drawn to the limitations of liability, indemnification and jurisdictional