NED National Endoscopy Database

# National Endoscopy Database

## Caldicott and data governance information

Part of the JAG programme at the RCP

JAG Joint Advisory Group on GI Endoscopy

Royal College of Physicians

# 1. Information for NED leads

To continue uploading data from your local endoscopy reporting system to the National Endoscopy Database, you will need to renew or obtain local approval. The minimum local approval required is Caldicott Approval. Further approval such as a Data Sharing Agreement (DSA) may be required according to local arrangements. In some organisations, the following approvals have been required and you should check with the appropriate departments if this is necessary in your organization:

- Audit department approval
- IT department approval
- Change control approval

**Please use the information below and the specimen Caldicott application below to aid local application for Caldicott approval in your organization.**

**Please inform the NED project team (askjag@rcp.ac.uk) when you have obtained Caldicott approval or if you have any queries.**

Formal agreement for continued engagement with the NED project should also be obtained from your endoscopy lead and endoscopists in the organisation. Usually, this is best addressed via the Endoscopy User Group or equivalent.

All participating endoscopists will be required to be registered on the JAG Endoscopy Training System (JETS). Endoscopists may 'opt out' from having their GMC or NMC number linked to their performance data, though they should be reassured that there will be clear restrictions on who can see their data. Endoscopists should be made aware of this option by the NED lead.

Caldicott approval is needed to allow export of data from the trust/organisation to the national database regardless of whether the data is patient identifiable or not. All NED data is patient non identifiable.

# 2. Supporting information for Caldicott Guardians of organisations participating in the National Endoscopy Database (NED)

## a. What is the purpose of the National Endoscopy Database (NED)?

The NED has been established in order to:

- pool endoscopy data from individual units around the UK
- enable quality assurance and benchmarking of standards
- deliver feedback to individual endoscopists and units with regards to their performance
- enable performance to be audited against current BSG and JAG quality standards
- act as a database for service evaluation and research
- automatically provide data for some of the current JAG audits

The aim is that by accurately measuring endoscopy performance and enabling benchmarking the quality of endoscopy will improve

## b. NED data and systems

1. Data controller
   The data collected by the National Endoscopy Database (NED) on behalf of the Joint Advisory Group on GI Endoscopy (JAG) and is owned by the Royal College of Physicians (RCP)
2. Data collection
   The data collected will not contain patient identifiable data. It will be procedural and will link data to clinicians and to services.
3. Data use
   The data inputs and outputs of the NED are under the auspices of the NED committee.
4. Application for access to the data beyond use by the JAG will need to be made to and approved by JAG clinical leadership.
5. Data governance
   The data listed should be used in accordance with the NED privacy policy.
6. Roles and responsibilities

| | |
|---|---|
| Data controller | The RCP |
| Database supplier | Weblogik |

## c. Scope and system of data collection NED

The NED is populated by data extracted automatically from the endoscopy reporting system (ERS) at endoscopy services in the UK. NED makes data available in user friendly outputs for clinicians, services and for research purposes. The aim of NED is to support and enable improved quality assurance in endoscopy, to enhance JETS (JAG Endoscopy Training System), removing the need for double data-entry for trainees and to offer potential for research by providing a central store of key endoscopy data.

Minimum patient data is used; only age and sex is recorded, as this is clinically relevant data to enable quality assurance. Each procedure is given a unique identifier in the National Endoscopy Database that contains a string of information to allow the procedure to be identified in the local endoscopy database for data quality checking purposes and to facilitate further service evaluation. Individuals and units receive feedback of their performance data.

## d. Patient consent

Patients will not be contacted or consented as data will not be made identifiable. Individual patient consent is not required. At the outset of NED in 2013 this position was clarified with the Confidentiality Advisory Group (CAG). In 2023, the UK Caldicott Guardians Council clarified that the data is not personal and not special category data, it is data collected in the healthcare space that is de-identified.

## e. Access to data

Access to the data by the NED office and clinical team and the database supplier/ administrators will be limited to individuals approved by the chair of the NED committee. This access will be for administrative purposes only.

A hierarchy of access to NED data was set up to restrict access:

- **NED admin** – This is the basic admin role for internal JAG users, giving the full access to NED and to make changes.
- **Endoscopist** – Standard role for all, this is needed for access to JETS portfolio and NED data. Without this role, no data will show for endoscopists if they log in to NED.
- **NED trust admin** – Access to whole trust data, able to see endoscopists at the trust by name and extract Audit reports.
- **Service lead** – Access to single site data. Able to see endoscopists by name and extract audit report. Typically used for independent sites.
- **NED supplier** – NED supplier access for ERS software companies – Gives access only to the Upload Success Rate for their sites.
- **Endoscopy network lead** – Access to trust level data in a specific region, endoscopist level data will not be accessible.
- **National lead** – Access to trust level data in a specific country, endoscopist level data will not be accessible.
- **Regional access** – Access to trust level data only for Endoscopy networks

Users can view performance data via the NED web site. This is similar in format to the existing JETS e-portfolio facility.

## f. Data storage

The application and database systems are operated by Weblogik Ltd, details of the environment are described below:

**Access to NED**: Access to the NED site is via a username/password combination with role based permissions controlling appropriate access to the data. User authentication is provided by Microsoft Azure B2C Active directory. Connection to the NED website is over SSL (2048 bit). Access to the NED upload service (also over SSL) requires a username and password for each unit.

**Hardware:** The NED/JETS application is hosted on a dedicated multi-tier environment accessed via the public internet behind a firewall device. The device provides: Anti Malware/intrusion prevention, advanced threat protection and anti spam services. Servers are running Windows Server 2022 and are maintained by a dedicated support team over a VPN connection. Data is encrypted at rest using self encrypting hard drives (SED) and SQL Servers Always Encrypted feature.

**Hosting Environment:** This environment is housed in a secure data center rack located in London Docklands, the NED environment is hosted on physical servers within this rack. The data centre offers high levels of data and network security, with electrical and mechanical systems engineered with multiple levels of redundancy, and 24x7 protection against fire and natural disasters.

**Physical Security:** The data centre has 24x7 security systems. Customers have the protection of security barriers, 24x7x365 monitoring by on-site personnel to include verification of all persons entering the building, CCTV video camera surveillance throughout, and security breach alarms.

**Access:** Access to the buildings, data floors and individual areas are via individually programmed access cards, and visual identification. Whenever you swipe your card tag over the sensors to gain access to the building, your digital photograph is displayed and on-site technicians verify the request before allowing access. Standardised procedures ensure you and your nominated staff can gain access to your equipment whenever you require, day or night.

**Power:** Customers have access to a redundant high-capacity power supply, scalable for future expansion. Power is isolated between customers, and with Uninterruptible Power Supply (UPS) systems and stand-by diesel generators on site to ensure a resilient location for important infrastructure equipment.

**Fire detection/suppression:** Very Early Smoke Detection Apparatus (VESDA) is installed in every facility. These highly sensitive smoke detectors, which are linked to the Building Management System and monitored continually from a network operations centre, provide very early detection to help avoid fire, loss and business disruption. This is coupled with an environmentally-friendly gas-based or water mist fire suppression system to put out fires, with minimal damage to equipment.

**Air Conditioning:** To ensure performance and avoid equipment failure, all data floors are managed such that air entering customers' equipment is maintained at a controlled temperature and relative humidity.

**Building Management System (BMS):** All facilities operate computerised Building Management Systems that monitor and remotely operate sensors covering electrical, mechanical, fire detection and leak detection systems.

**Backups:** The system is backed up each day using Microsoft Data Protection Manager with transaction log shipping every 15 minutes.

## g. Requests for external and research access to NED

Requests for external and research access to anonymised NED data will be overseen by JAG clinical leadership and the JAG programme manager (data and training).

# Appendix 1: Specimen Caldicott application form

## Use and release of personal identifiable data (Caldicott approval form)

Introduction

The purpose of the request for use or release of person-identifiable data form is to record the details of identifiable information sent from the Trust/organization to other partners/agencies. This will ensure that all data flows of personal and/or sensitive information, including healthcare, medical and non-medical, are conducted in a secure and confidential manner and approved by the Caldicott Guardian where necessary.

| |
|---|
| **Description of proposal:**<br><br>The National Endoscopy Database (NED) is populated by data extracted automatically from the endoscopy reporting system (ERS) at endoscopy services in the UK. NED makes data available in user friendly outputs for clinicians, services and for research purposes. The aim of NED is to support and enable improved quality assurance in endoscopy, to enhance JETS (JAG Endoscopy Training System), removing the need for double data-entry for trainees and to offer potential for research by providing a central store of key endoscopy data. |
| **Is the data being sent externally?**<br><br>**Yes:** ☐ **No:** ☐ |
| **Time period for data required:**<br>**Start date: March 2025** **End date: indefinite**<br><br>**Please state regularity: rolling upload** |
| **Receiving organisation/individual**<br><br>**Organisation name: National Endoscopy Database**<br><br>**Address: Royal College of Physicians London, 11 St Andrews Pl, London NW1 4LE**<br><br>**Appointed person responsible for data: Dr Tom Lee**<br><br>**Contact details: as above** **Email address:** askjag@rcp.ac.uk |
| **Recipients location for receiving and processing data:**<br><br>**NHS Organisation** ☐ **Government Dept.** ☐ **UK** ■<br><br>**EEA Country** ☐ **Non EEA Country** ☐ |
| **Who else will have access to the data?**<br>**(*If data recipients are not employed by the NHS please state whether NHS honorary contracts are in place. If not – detail confidentiality agreements.)*** |

**Method of secure information / data transfer (please tick):**

| | | | | | |
|---|---|---|---|---|---|
| **NHSmail.net** | ☐ | **Secure fax** | ☐ | **Removable media encryption AES 256** | ☐ |
| **Email (secured)** | ☐ | **Special Delivery / courier** | ☐ | **Electronic File Transfer** | ■ |

**Organization Safe Haven ……**

**Please describe the applicable security arrangements for the transfer:**

**Access to NED**: Access to the NED site is via a username/password combination with role based permissions controlling appropriate access to the data. User authentication is provided by Microsoft Azure B2C Active directory. Connection to the NED website is over SSL (2048 bit). Access to the NED upload service (also over SSL) requires a username and password for each unit.

**Hardware:** The NED/JETS application is hosted on a dedicated multi-tier environment accessed via the public internet behind a firewall device. The device provides: Anti Malware/intrusion prevention, advanced threat protection and anti spam services. Servers are running Windows Server 2022 and are maintained by a dedicated support team over a VPN connection. Data is encrypted at rest using self encrypting hard drives (SED) and SQL Servers Always Encrypted feature.

**Hosting Environment:** This environment is housed in a secure data center rack located in London Docklands, the NED environment is hosted on physical servers within this rack. The data centre offers high levels of data and network security, with electrical and mechanical systems engineered with multiple levels of redundancy, and 24x7 protection against fire and natural disasters.

**Physical Security:** The data centre has 24x7 security systems. Customers have the protection of security barriers, 24x7x365 monitoring by on-site personnel to include verification of all persons entering the building, CCTV video camera surveillance throughout, and security breach alarms.

**Access:** Access to the buildings, data floors and individual areas are via individually programmed access cards, and visual identification. Whenever you swipe your card tag over the sensors to gain access to the building, your digital photograph is displayed and on-site technicians verify the request before allowing access. Standardised procedures ensure you and your nominated staff can gain access to your equipment whenever you require, day or night.

**Power:** Customers have access to a redundant high-capacity power supply, scalable for future expansion. Power is isolated between customers, and with Uninterruptible Power Supply (UPS) systems and stand-by diesel generators on site to ensure a resilient location for important infrastructure equipment.

**Fire detection/suppression:** Very Early Smoke Detection Apparatus (VESDA) is installed in every facility. These highly sensitive smoke detectors, which are linked to the Building Management System and monitored continually from a network operations centre, provide very early detection to help avoid fire, loss and business disruption. This is coupled with an environmentally-friendly gas-based or water mist fire suppression system to put out fires, with minimal damage to equipment.

**Air Conditioning:** To ensure performance and avoid equipment failure, all data floors are managed such that air entering customers' equipment is maintained at a controlled temperature and relative humidity.

**Building Management System (BMS):** All facilities operate computerised Building Management Systems that monitor and remotely operate sensors covering electrical, mechanical, fire detection and leak detection systems.

**Backups:** The system is backed up each day using Microsoft Data Protection Manager with transaction log shipping every 15 minutes.

**How will the service users be contacted? No contact will be made**

**What information will be given to the service user about the purpose? none**

**How will the service users consent be obtained?**
Patients will not be contacted or consented as data will not be made identifiable. Individual patient consent is not required. At the outset of NED in 2013 this position was clarified with the Confidentiality Advisory Group (CAG). In 2023, the UK Caldicott Guardians Council clarified that the data is not personal and not special category data, it is data collected in the healthcare space that is de-identified.

**How long will the data be stored? indefinitely**

**Where will the data be physically stored: see above**

**If the data is on a computer is there access via a local network or the internet?**
**See above**

**How will data be protected? (Please detail security measures to be taken)**
**See above**

**At the end of this period how will the data be disposed?**
**No plans made to dispose of data.**

**You must address the 8 Caldicott Principles – please give a brief description under each of the following headings**

| |
|---|
| **Principle 1** - **Justify the purpose(s) for using confidential information**<br>Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.<br><br>National collection of endoscopy data to improve quality assurance of endoscopy |
| **Principle 2** - **Use confidential information only when it is necessary**<br>Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.<br><br>Only age and gender will be uploaded. No other patient identifiable information will be retrieved. Each procedure will be given a unique identifier in the National Endoscopy Database that will contain a string of information to allow the procedure to be identified in the local endoscopy database for data quality checking purposes and to facilitate further service evaluation. |
| **Principle 3** - **Use the minimum necessary confidential information**<br>Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.<br><br>Only age and gender are required. These are clinically relevant data which will contribute to the quality assurance process. |
| **Principle 4 - Access to confidential information should be on a strictly need-to-know basis**<br>Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.<br><br>Only national clinical leads, database managers and individuals approved by the chair of the National Endoscopy Database committee and the project team will be permitted access to data. |
| **Principle 5** - **Everyone with access to confidential information should be aware of their responsibilities**<br>Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.<br><br>All individuals involved in the project will be aware of their responsibilities.<br>Individual organizations providing data to the national database will be required to obtain local information governance and Caldicott approval where appropriate |
| **Principle 6** - C**omply with the law**<br>Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.<br><br>The project team will be responsible for ensuring legal requirements are fulfilled. |
| **Principle 7 - The duty to share information for individual care is as important as the duty to protect patient confidentiality** |

Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

The National Endoscopy Database aims to contribute to improvements in the quality of endoscopy in the United Kingdom. This is facilitated by pooling anonymised endoscopy data to produce key performance indicators for benchmarking and quality improvement purposes. The information governance arrangements support Trusts uploading data to NED once Caldicott approval has been obtained locally. NED data will not be shared outside these arrangements.

**Principle 8 - Inform patients and service users about how their confidential information is used**
A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

A leaflet will be provided for all services participating which should be displayed in patient areas.

I can confirm that I'm happy to share data according to the terms and information given as described within this approval form.

Name: Title:

Signature: Date:

If the form has been completed by a Medical Student or other similar training posts a supervisory signature or equivalent is required below:

Name: Title:

Signature: Date:

Further information regarding this report may be obtained from the JAG office at the Royal College of Physicians.

JAG office
Accreditation Unit
Royal College of Physicians
11 St Andrews Place
London
NW1 4LE

askJAG@rcp.ac.uk

www.thejag.org.uk

www.ned.thejag.org.uk

The publication is copyrighted to the Royal College of Physicians of London. The named service on the front page of this report may reproduce all or part of this publication, free of charge in any format or medium provided. The text may not be changed and must be acknowledged as copyright with the document's date and title specified. All images and logos contained within this report cians.