NED Data Protection Impact Assessment (DPIA)

Document control:

	Name and role	Contact details
Document Completed by	Raphael Broughton, Senior Programme Manager, JAG	Raphael.broughton@rcplondon.ac.uk
Data Protection Officer name	Pamela Forde, RCP data protection officer.	dataprotection@rcplondon.ac.uk
Document approved by	RCP Care Quality Improvement Department, Information Governance Committee	dataprotection@rcplondon.ac.uk

Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	Z7085833
	Date registered:
	    17 September 2002
	Data controller:
	    ROYAL COLLEGE OF PHYSICIANS OF LONDON
	Address:
	    11 ST ANDREWS PLACE
	    REGENTS PARK
	    LONDON
	    NW1 4LE

Date Completed	Version	Summary of changes
October 2018	V0.1	HC created and added core info
December 2018	V0.2	RB updated to present questions to CQID data protection group
February 2019	V0.3	Amendments made following TC comments
February 2019	V0.4	Document diagram updated and sign off from NED committee
May 2019	V1.0	Final version approved by RCP CQID information governance committee

2. Screening questions checklist

No.	Question	Yes/no	Comments
1	Does your project involve any automated decision making, evaluation or scoring including profiling and predicting using information about a person?	No	The primary function of NED involves the automatic extraction of KPI data from a services local reporting systems (ERS) pertaining to individual endoscopists. For individual endoscopists who have decided to opt-out, their data will still be uploaded but anonymised (i.e. their GMC number will not be uploaded however procedural data will be uploaded and anonymised). Please note, the outcome of this project does not directly determine a services right to perform endoscopy or apply/maintain JAG accreditation.
2	Does your project involve any sensitive information or information of a highly personal nature?	No	NED collects patient age and gender, but no patient identifiable data (eg date of birth) is collected. NED collects endoscopist level data including GMC/NMC/HCPC number and procedural performance data. The registration number can be used to identify the individual endoscopist's name and gender which is publicly available.
3	This group may include children, employees, mentally ill persons, asylum seekers, or the elderly, patients and cases where there is an imbalance in the relationship between the position of the individual and the controller.	Yes	Data about individual endoscopists (GMC/NMC/HCPC number and procedural data) is uploaded regardless of patient age or other criteria. Data about individual endoscopists will be uploaded from procedures completed on those who are under 16 years old.
4	Does your project involve any innovative use or applying new technological or organisational solutions? This could include biometric or genetic data, the tracking of individuals' location or behaviour?	No	Uploading data to NED may require modifications to be made to a services' local endoscopy reporting system (ERS), these may involve adding additional data fields, but this is not new technology.
5	Does your project match data or combine datasets from different sources?	No	Data is only taken from one source. Data is extracted from the endoscopy

			reporting system and matched via registration number (e.g. GMC/NMC/HCPC number) to link it to an individual in NED. NED data is also accessible via the JAG Endoscopy Training System (JETS).
6	Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	No	Data is automatically extracted from the local reporting system. Endoscopists are not advised at point of entry that data (related to their registration number and procedural performance data) will be extracted to NED. Endoscopy services confirm Caldicott Guardian approval for data to be shared with NED prior to data being collected. This approval specifies that the data being shared is non-identifiable patient information. All services have been informed about NED and how their data will be recorded. The endoscopy lead within the service cascades information internally. There is a publically available patient information leaflet which is available on the NED website.
7	Does your project process data that might endanger the individual's physical health or safety in the event of a security breach?	No	Project is limited to data extraction and presentation to clinical teams about the quality of services.
8	Is this a new project? Or have the requirements for your project changed since its initiation? Are you sharing new information or linking to new datasets that were not part of the original project specification. Have you added any new audit streams to your project?	No	This project was first conceived in 2013, and the database been active since 2015. Since the original specification, there have been no amendments to the dataset collected or additional data linkages.

Project aims

Overseen by the Joint Advisory Group on Gastrointestinal Endoscopy (JAG), The National Endoscopy Database aims to help improve endoscopy quality in the UK

The NED will be used to identify high-performing and underperforming endoscopy units and will look for correlations with both the trust post-colonoscopy CRC (PCCRC) rates, and the JAG accreditation Global Rating Scale.

Unwarranted variation in colonoscopy quality is life threatening, and at present we do not know the extent of variation in endoscopy quality in the UK. Local ad-hoc audits are non-standardised and often methodologically flawed which means that there's currently no sufficient way to easily identify underperformance and intervene. In the UK, 41, 000 people a year are diagnosed with Colorectal cancer (CRC). Considering CRC arises from polyps, colonoscopic polyp detection and resection is pivotal in CRC prevention. 500, 000 colonoscopies are performed in the UK each year and low "polyp-detecting" colonoscopists have higher post-procedure CRC incidence and mortality rates. The newly discovered serrated CRC pathway is now thought to account for 15-30% of CRC's. This occurs predominantly in the proximal colon and is likely to explain why proximal CRCs are missed over twice as often as distal CRCs. The NED will aim to improve the accuracy of pathology detection by striving to determine optimal proximal colon detection KPI.

Project objectives

- The NED project aims to improve the accuracy of pathology detection by striving to determine optimal proximal colon detection KPI.
- The NED will be used to identify high-performing and underperforming endoscopy units and will look for correlations with both the trust post-colonoscopy CRC (PCCRC) rates, and the JAG accreditation Global Rating Scale.

Data processing

The data storage and database systems will be run by an IT provider - Weblogik. The data storage details are described below:

Access to NED

Access to the NED/JETs site is via a username/password combination (stored as one way hash) and is over SSL (2048 bit). Access to the NED upload service is also over SSL and requires a username and password for each unit as well as a unique supplier identifier. Servers are running Windows Server 2008 software.

Hardware

The NED/JETS application is hosted on a multi-tier environment accessed via the public internet behind a CISCO firewall.

Hosting Environment

Weblogik has its own secured rack within the Digital Realty data centre at London Docklands, the NED application is hosted on multi-tier 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 Digital Realty Group facilities operate computerised Building Management Systems that monitor and remotely operate sensors covering electrical, mechanical, fire detection and leak detection systems.

Backups

The application is backed up each day to an onsite NAS (Network Attached Storage device), transaction level backups are taken every 15 minutes and full backups once a day to a separate off site NAS. These backups are performed over a VPN and are stored in a locked server cabinet within Weblogik's main office. The office is in a secure compound, protected by CCTV, requiring access cards to gain entry (at multiple points); the office itself is protected by a monitored alarm system.

Publishing your DPIA report

Publishing a DPIA report is not a legal requirement but you should consider publishing this report (or a summary or a conclusion) and you should send it to your stakeholders. Publishing the DPIA report will improve transparency and accountability, and lets individuals know more about how your project affects them. Though there may be a need to redact/remove sensitive elements e.g. information on security measures.

State in the box below if you are going to publish your DPIA. If so, please provide hyperlink to the relevant webpage if this has been done already or insert the date you intend to publish it.

> Latest version will be publicly available on NED website -
> https://ned.jets.nhs.uk/KPI/Default.aspx?ContentId=ServiceDocumentation

Data sharing and security

Data sharing	
Will the data be shared with any other organisations? If yes, please list the names of the organisations	Yes data is shared with various levels of access and permissions to the following: - Endoscopy services - Endoscopists - NHS Improvement – Getting it right first time project team - Newcastle University - Durham University - Northumbria University The shared data consists of: - non patient identifiable data – NED will only capture age and gender - Registration numbers (GMC and NMC) - Key Performance Indicators (KPI's)
How will the data be shared?	The NED operates with a hierarchy of access: **Individual endoscopists:** Access to all data assigned to their individual GMC/NMC. They can therefore access their own data from across all the sites they work at, even if some sites sit outside their main trust (cross-organisation data). **Organisation (trust or equivalent)/ service leads**: Access named data relating to procedures completed within their organisation or service. To obtain this level of access email askjag@rcplondon.ac.uk Organisation and service leads can only see procedures completed at their organisation or service. E.g.if a clinician did procedures at an NHS trust and a private provider, the lead at the NHS trust would only see the NHS data. **National level:** Data will be used for quality assurance by JAG as part of the JAG accreditation programme. This data will include named hospitals but anonymous endoscopists. Anonymised data **(without endoscopists names)** will be available for research. Access to data for research purposes is governed by JAG research committee and RCP's information governance groups. JAG office administrative team can also

| | access data to support users to answer queries relating to their accounts.

Whether or not a service is participating in NED, the date of the first upload and the number of procedures will be shared with NHS Improvement – Getting it right first time (GIRFT) project team. No procedural data or other information is being shared with the GIRFT team. There is a DSA in place to secure this.

Endoscopy service level, pseudo anonymised data will be shared with Newcastle, Durhan and Northumbria universities as part of the NED APRIOQT research project, which seeks to identify an improved indicator for endoscopy performance. This data will not include endoscopist name or membership number. |
|---|---|
| Are there any information sharing agreements or protocols in place to support the sharing of data? If so, please provide a copy. | Yes

If shared outside of JAG/RCP a data sharing agreement will be in place.

Data is shared with Newcastle university as part of the NED APRIQOT project. |

Data security

What security measures have been undertaken to protect the data?	Physical security & hierarchy of access as described above
What business continuity plans are in place in case of data loss or damage (i.e. as a result of human error, virus, network failure, theft, fire, floods etc).	Data Loss NED Database is backed up using Microsoft Data Protection Manager off site

Virus Anti-virus protection used on workstations and servers signatures updated automatically. Workstation and Server OS/Applications regularly patched.

Theft/Fire/Floods/Power Servers located in secure data centre, with multiple physical security access controls, N+1 Power redundancy, Fire Detection and suppression.

Human Error Data loaded automatically system to system without intervention. Access controls and auditing in place for who can access the underlying databases.

Network Failure |

	IP Transit is multi homed IP Hacking Office and hosted environment protected by firewalls In Event of a disaster Current DR plan provides restorations of services within 1 working day. ERS system uploads would fail whilst the service is down, and once available again they will resend the procedures which have failed upload
Does the system or process / policy involve changing the standard disclosure of publicly available information in such a way that the data becomes more readily available than before?	See hierarchy of access answer above
What is the data retention period for this data? (please consult the detailed retention schedule (appendix 3) in the link below https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016)	50 years As it is procedural information it may be relevant to clinician throughout their consultant career. Also historic dataset will useful for longitudinal research studies.
How will the data be securely destroyed when it is no longer required?	IT provider will delete historic data in line with retention period.

Data Information Flow

Please describe how personal information is collected, stored, used and deleted. Use your data flow map and information asset register to help complete this section. Explain what personal information is used, what it is used for, who it is obtained from and disclosed to, who will have access and any other necessary information. Completing this section can help identify potential 'function creep', unforeseen or unintended uses of the data for example data sharing.
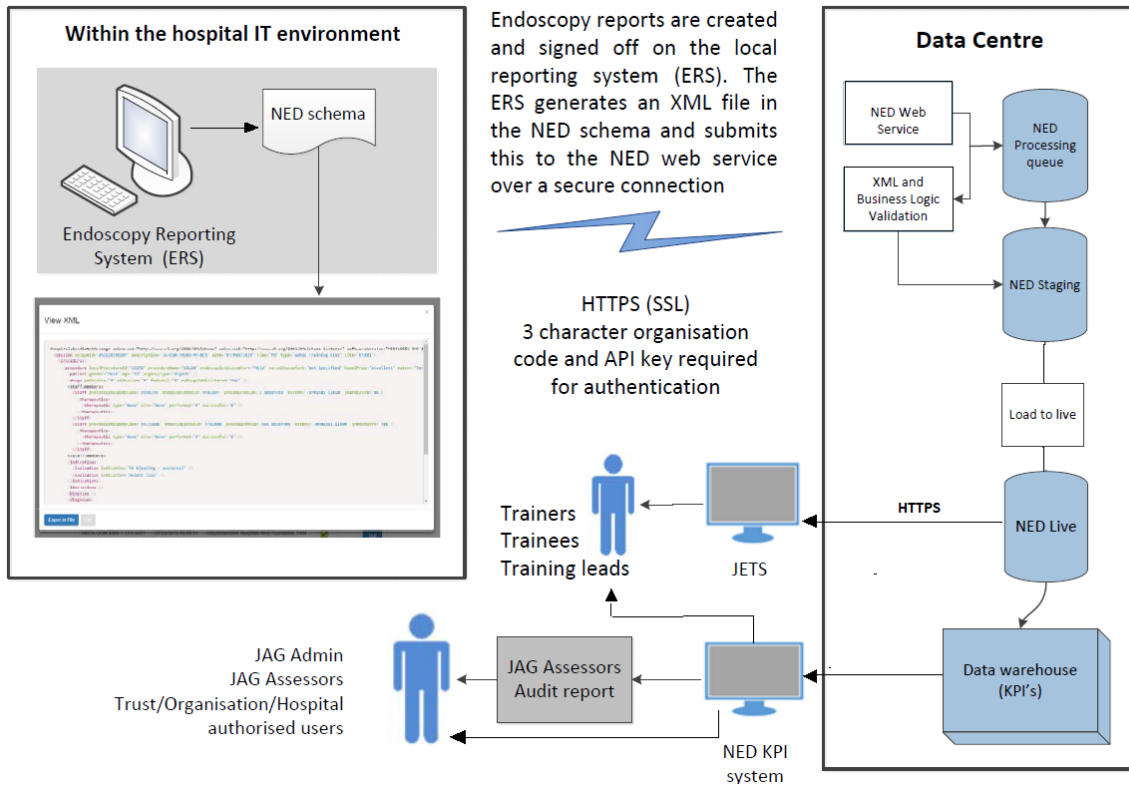
Transferring personal data outside the European Economic Area (EEA)

If personal data is being transferred outside of the EEA, describe how the data will be adequately protected (e.g. the recipient is in a country which is listed on the Information Commissioner's list of "approved" countries, or how the data is adequately protected).

No personal data is transferred outside of the EEA.

Privacy Risk Register
Justification for collecting personal data

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. In certain circumstances it may be unlawful to process information not described in the transparency information (privacy notice/fair processing material) which informs individuals how their personal data is being used.

It may not be necessary to process certain data items to achieve the purpose. They may be irrelevant or excessive leading to risk of non-compliance with the Data Protection Act.

In the tables below list and justify personal data items needed to achieve the lawful aim of a project that requires information on individuals and their personal characteristics. Insert as many more lines that you need. Work through the table of items and decide whether or not you should be collecting the information, examine each data field and decide if you need it. There are two sections in the table below, one for personal data and one for personal sensitive data items.

Data Categories [*Information relating to the individual's*]	Is this field used?	N/A	Justifications [*there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project*]
Personal Data			
Name	Yes	N/A	Endoscopist name is recorded to make data effective for local quality assurance i.e. identifying who data belongs to.
NHS number		N/A	
Address		N/A	
Postcode		N/A	
Date of birth		N/A	
Date of death	Yes		If a patient were to die during a procedure, this would be recorded as an adverse event. It would be linked to endoscopist, but not to patient.
Age	Yes		Patient age is recorded as certain KPIs only apply to certain age groups e.g. recommended drug doses administered to patients are dependent on patient age. Also it is recorded to help determine commonalities in terms of the correlation between age and diagnoses.
Sex		yes	See gender
Marital Status		N/A	
Gender	Yes		Patient gender is recorded to assist with research and also to support quality assurance of endoscopy services as certain symptoms/ diagnosis are more likely for certain genders. Having information on gender will enable the endoscopists to better identify trends and their performance.

Data Categories [*Information relating to the individual's*]	Is this field used?	N/A	Justifications *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Living Habits		N/A	
Professional Training / Awards		N/A	
Income / Financial / Tax Situation		N/A	
Email Address	Yes		Endoscopist email address is held in NED. This is used for communication with users. The email address is not uploaded from local ERS, it is housed in NED user account. No patient identifiable or contact information is recorded.
Physical Description		N/A	
General Identifier e.g. Hospital No		N/A	
Home Phone Number		N/A	
Online Identifier e.g. IP Address/Event Logs		N/A	
Website Cookies		N/A	
Mobile Phone / Device No		N/A	
Device Mobile Phone / Device IMEI No		N/A	
Location Data (Travel / GPS / GSM Data)		N/A	
Device MAC Address (Wireless Network Interface)		N/A	
Sensitive Personal Data			
Physical / Mental Health or Condition		N/A	
Sexual Life / Orientation		N/A	
Family / Lifestyle / Social Circumstance		N/A	
Offences Committed / Alleged to have Committed		N/A	
Criminal Proceedings / Outcomes / Sentence		N/A	
Education / Professional		N/A	

Data Categories [Information relating to the individual's]	Is this field used?	N/A	Justifications [there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]
Training			
Employment / Career History		N/A	
Financial Affairs		N/A	
Religion or Other Beliefs		N/A	
Trade Union membership		N/A	
Racial / Ethnic Origin		N/A	
Biometric Data (Fingerprints / Facial Recognition)		N/A	
Genetic Data		N/A	

As well as above, procedural data is recorded. This is linked to individual endoscopist.

ICO guidance/advice on DPIA's

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

DPIA process checklist

✓ We describe the nature, scope, context and purposes of the processing.

✓ We ask our data processors to help us understand and document their processing activities and identify any associated risks.

✓ We consider how best to consult individuals (or their representatives) and other relevant stakeholders.

✓ We ask for the advice of our data protection officer.

✓ We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure data protection compliance.

✓ We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.

✓ We identify measures we can put in place to eliminate or reduce high risks.

✓ We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.

✓ We implement the measures we identified, and integrate them into our project plan.

✓ We consult the ICO before processing, if we cannot mitigate high risks.

✓ We keep our DPIAs under review and revisit them when necessary.