

# NVR Privacy Notice, Independent Providers Pilot

## What is the aim of the National Vascular Registry?

The National Vascular Registry (NVR) was established in 2013 to measure the quality and outcomes of care for patients who undergo major vascular procedures in NHS hospitals, and to support vascular services improve the quality of care for these patients by publishing high-quality benchmark information. The NVR was commissioned by the Healthcare Quality Improvement Partnership (HQIP) as part of the National Clinical Audit and Patient Outcomes Programme (NCAPOP).

Hospital-based vascular services treat patients with conditions that affect blood circulation, and which are part of the broad spectrum of cardiovascular disease. The treatments for these conditions are typically aimed at reducing the risk of cardiovascular events such as a heart attack, stroke or the rupture of an artery.

In 2021 the NVR embarked on a pilot project to establish the feasibility of collecting data from private patients being treated in independent hospitals in England and Wales. Previously the NVR was only limited to NHS hospitals.

## Where is patient data collected from?

The NVR captures data on adult patients undergoing emergency and elective procedures in NHS hospitals for the following patient groups:

1. patients who undergo carotid endarterectomy or carotid stenting
2. patients who have a repair procedure for abdominal aortic aneurysm (AAA), both open and endovascular (EVAR)
3. patients with peripheral artery disease (PAD) who undergo either (a) lower limb angioplasty/stent, (b) lower limb bypass surgery, or (c) lower limb amputation.

## Data Controller

The NVR is commissioned by the [Healthcare Quality Improvement Partnership \(HQIP\)](#) as part of the National Clinical Audit Programme on behalf of NHS England and the Welsh Government. HQIP are the data controllers for the private patient data submitted to the audit directly by independent hospitals in England and Wales

## Legal basis under the common law duty of confidentiality

In this independent hospitals pilot, all UK resident private patients being treated in England and Wales and are required provide consent for their personal identifiable information to be collected on the NVR. Patients who are not UK residents are not to be included in this pilot.

## Legal basis for processing personal patient data

The NVR processes data under articles 6 (1) (f) and 9 (2) (h) of the GDPR as the data are needed under the legal basis of legitimate interest to assess the provision and management of health or social care systems.

## How we protect your patient data

Local clinical teams enter patient data into a secure web-based tool provided by Northgate Public Services. Only doctors, nurses and clinical audit staff registered with the NVR can access the data collection tool. Security and confidentiality is maintained through the use of passwords and a person specific registration process. Only the NVR project team can manage access to the data collection tool.

## Patient confidentiality and level of data collected

The patient information received and managed by the NVR team is treated as confidential. We analyse the data to produce the information on patient care and outcomes, the NVR team use de-identified data and so individual patients are not identifiable.

The audit is also careful when publishing information to include graphs or tables that do not allow individuals to be identified. To ensure this, the Audit follows guidelines on publishing statistics issued by the Office for National Statistics – [Review of the Dissemination of Health Statistics: Confidentiality Guidance](#).

## Management of patient data by the NVR team

The NVR team are based at the Royal College of Surgeons of England (RCSEng). The RCSEng conforms to the General Data Protection Regulation (GDPR) and other legislation that relates to the collection and use of patient data. The RCSEng has strict security measures in place to safeguard patient information held in the Data Collection system and when analysing NVR data. The NVR data that can be extracted by the NVR team for analysis is de-identified as it doesn't include patient names or NHS numbers. The full date of birth is automatically converted to age and month and year of birth. The full patient postcode is converted to something called lower super output area (LSOA) which only uses the first half of the postcode plus the next number. These de-identified datasets will be held by the NVR team as long as they remain the contract holder of the National Vascular Registry – currently up until 31st December 2022.

The Data Collection IT system has various levels of security built into it, such as ID password security, which prevents unauthorised users gaining access and data encryption. The full patient identifiable dataset will remain on the NVR IT system with the rest of the NHS patient data.

## Who we share data with?

The NVR only shares patient-level data following a strict governance procedure to ensure compliance with the General Data Protection Regulation (GDPR).

The NVR is linked to the AAA screening programme IT System in England. As the NVR and these Screening Programmes are both hosted by Northgate, patient identifiers are securely transferred

between the two systems. This is done each day in the early hours of the morning. If a man is found to have a AAA via the national screening programme, is referred for surgery, and has given consent for his data to be used, then the NHS number is shared with the NVR. Once the patient record is created and submitted on the NVR, details of the operation are automatically shared back to the man's record on the screening programme IT system.

De-identified patient data collected as part of this private hospitals pilot will not be shared with researchers for secondary purposes. For the data collected in the NHS, researchers may apply to the NVR Data Controller (HQIP) if they want to use it for secondary purposes, such as a clinical audit, service evaluation, or a research study. These requests undergo a stringent approvals process as outlined on the [HQIP website](#).

## What if I do not want my information used by the Audit?

If you do not want your personal identifiable information to be used in the Audit, please tell the people who are treating you. They will make sure this information is not used in the audit.

Your specific rights are:

- See the information we hold on you, and confirm what data we are processing about you.
- Be informed about the collection and use of your personal data.
- Ask us to correct any inaccurate, out of date or incomplete personal data.
- Request that we erase the personal information we hold on you. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.
- Request that we restrict or limit the way that we use your personal data.
- Request a copy of your information and where possible we will provide it to you in a machine-readable format such as .CSV file if you wish. We will do this free of charge and would include only the information you have provided directly to us.
- Object to the processing of your information.

If you provide consent to the team performing your procedure to record your data on the NVR and then change your mind, please send an [nvr@rcseng.ac.uk](mailto:nvr@rcseng.ac.uk) and put "Request to opt-out" in the subject line. On receipt of your email, we will remove your personal details from the NVR IT system. Alternatively, you can notify a member of your local care team that you wish to opt out. They will then ensure that your personal details are removed from the Registry.

You are also able to opt-out of the NVR using your personal data for linkage with other NHS data sources if applicable, such as HES, by registering your preference in the [National Data Opt-Out](#) policy, which is managed by NHS Digital.

## Changes to our privacy policy

We keep our privacy policy under regular review and we will always include the latest version on this web page.

The privacy policy was last updated on 03/09/2021

## How to contact us

Please [contact us](#) if you have any questions about our privacy policy or information we hold about you.

The Royal College of Surgeons of England has a data protection officer who can help you with any queries about the information in this privacy notice: [dpo@rcseng.ac.uk](mailto:dpo@rcseng.ac.uk)

HQIP also has a data protection officer and they can be contacted by email: [data.protection@hqip.org.uk](mailto:data.protection@hqip.org.uk)

Information about the requirements for the Audit to keep personal data secure and what to do to report a data breach, can be found on the website of the Information Commissioners Office: <https://ico.org.uk>

If you feel that your personal data has not been used correctly, please write to us in the first instance, so that we can do our best to correct this. Independently, you have the right to lodge a complaint with the [Information Commissioner's Office \(ICO\)](#), you can visit their website for information on how to make a data protection complaint.