SSNAP Fair Processing Statement

What we do with your data

The Sentinel Stroke National Audit Programme (SSNAP) aims to improve the quality of stroke care by measuring the structure, processes, and outcomes of stroke care against evidence based standards. These standards are informed by the National Clinical Guideline for Stroke, and national and local benchmarks. By reporting against these standards, stroke service providers can identify which aspects of their care need to be improved and put plans in place to achieve this so that more patients receive the best possible care available in the future.

The SSNAP team are located within the School of Population Health and Environmental Sciences at King's College London (KCL). The School of Population Health and Environmental Sciences conforms to the Data Protection Act and other legislation that relates to the collection and use of patient data, and has strict security measures in place to safeguard patient information. SSNAP stores pseudonymised patient data on a secure computer to which only authorised audit team members have access. The IT system has various levels of security built into it, including:

- ID password security: the data is stored on a password protected system, which prevents unauthorised users gaining access. Users are required to have a complex password that is set to expire after a given period. This ensures passwords are updated regularly.
- The stored data files are encrypted.
- All system database accesses are recorded in a system log file that can be audited in the event of suspected security threats or data misuse.

Why we need to collect and use your data

The SSNAP clinical audit collects data prospectively on all patients in England, Wales and Northern Ireland admitted to hospital following a stroke, from admission to 6 months after stroke. The webtool has been developed to measure against evidence based processes and outcomes of care. Collecting data on all stroke patients allows stroke service providers to identify methods of improving their care at a local, regional and national level. SSNAP's legal basis for processing patients' data under the General Data Protection Regulation (GDPR) is that the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (under Article 6 (1) (e)). This is justified as the commissioning arrangements link back to NHS England, Welsh Government and other national bodies with statutory responsibilities to improve quality of health care services.

Furthermore, the processing of sensitive patient data is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific

Version 5.0 (October 2020)

measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy (Article 9 (2) (i)). This is justified as SSNAP aims to drive improvements in the quality and safety of care and to improve outcomes for patients.

Patient level data are essential for meaningful data linkage. Data linkage is a process which combines together two or more sets of data from different organisations to produce valuable information which can be used for research and statistical purposes. Further details on data linkage are available below.

Who we share your data with outside KCL

Netsolving Ltd is subcontracted by SSNAP to collect and record patient information via their electronic webtool. More information about how Netsolving Ltd ensure patient data are kept safe and secure is available on their website http://www.netsolving.com.

SSNAP only share patient-level data following a strict governance procedure to ensure compliance with the Data Protection Act. SSNAP have permission to link patient-level data with other national databases on a case-by-case basis, only for the agreed purpose outlined in the section 251 agreement. As part of this process SSNAP must assure the confidentiality advisory group that SSNAP will use the patient information to improve patient care and serve the wider public interest. SSNAP holds current Data Sharing Agreements with NHS Digital and NHS Wales Informatics Service that grant permission for SSNAP to link data collected in England and Wales with Hospital Episode Statistics (HES), Patient Episode Database for Wales (PEDW), and Office of National Statistics (ONS) data. NHS Digital are the data controllers of HES and ONS data i.e. they are the organisation in control of processing the data. Linkage with HES and PEDW data enables SSNAP to compare the number of records submitted to SSNAP with the number recorded retrospectively in HES and PEDW to ensure high data quality. This linkage also enables analyses on the associations between stroke and other medical conditions. Linking with ONS data allows SSNAP to report all-cause mortality rates in the first 30 days after patients are admitted to hospital with stroke. Aggregate level mortality data is reported at hospital level annually and, once reviewed by all hospitals, are made available in the public domain.

The SSNAP team will not publish information that can enable individual patients to be identified, nor allow third-parties to access the patient identifiable data. The confidentiality and security of patient information will be maintained in the following ways:
- All reports are produced at an aggregate level (national, regional, hospital).
- In each audit publication, the statistical information is reviewed to ensure the risk of identification is minimised, and where necessary, small numbers are suppressed. This assessment follows guidelines issued by the Office for National Statistics - Review of the Dissemination of Health Statistics: Confidentiality Guidance (PDF).

Researchers may apply to SSNAP's data controller (the Healthcare Quality Improvement Partnership, HQIP), for access to selected variables in the SSNAP data. These requests undergo a stringent approvals process outlined here: https://www.hqip.org.uk/national-programmes/a-z-of-nca/audits-and-data-gov-uk/

How we protect your data outside the territories covered by the GDPR

All information managed by the SSNAP team is held and used within the UK. Patient level data is not shared outside the territories covered by the GDPR.

How long we keep your data and why

The patient information received and managed by the SSNAP team is treated as confidential. The information is available to the SSNAP team in a pseudonymised format, with individual patients only distinguished by a computer-generated sequence of numbers. Where an HQIP-commissioned programme was not extended, HQIP, as data controller, would usually request that all data collected is anonymised and returned to HQIP at the end of the contract. All data processors would be required to delete the data held at the end of the contract, unless agreed otherwise with HQIP, and appropriate permissions were in place.

Where we got your data from, if not you

Stroke patient data is submitted directly to SSNAP by clinical teams treating the patient. The data may be collected from hospital records, or collected specifically for the purpose of SSNAP.

SSNAP currently has approval under Section 251 to set aside the common law duty of confidentiality and collect confidential data about patients without explicit consent on the first six months of patient care (reference number: ECC 6-02(FT3)/2012) for all stroke patients admitted to hospital. More information on section 251 is available here: http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/what-is-section-251/ . The rationale for this is that many stroke patients are extremely unwell in the acute phase of their treatment and it is therefore not feasible to rely on patient consent during this time period. Data is collected by clinical teams via a secure web-based tool provided by Netsolving Ltd. Security and confidentiality is maintained through the use of passwords and a person specific registration process. SSNAP's funders the Healthcare Quality Improvement Partnership (HQIP) are the data controllers for the patient data submitted to the audit from England and Wales i.e. they are the organisation in control of processing the data. SSNAP reports aggregate level data at provider (hospital or community service) level and population level every quarter and on an annual basis.

Patient consent is explicitly sought by the clinical team treating the patient at six months post-stroke though it can also be recorded during the patient's inpatient stay. If a patient refuses consent for inclusion in SSNAP, all their personal identifiable information (e.g. name and NHS number) will be deleted from the dataset and no further linkages to other data sources will therefore be possible. However their non-identifiable data will continue to be held on the database as it is important for the purpose of SSNAP to analyse all data without selection bias. Opting out from SSNAP will not affect the care a patient receives. The SSNAP team do not have access to patient identifiable information at any point in the patient pathway.

By 31 March 2021, all healthcare providers in England must comply with the National Data Opt Out (https://digital.nhs.uk/services/national-data-opt-out). Patient data entered onto SSNAP is subject to the opt out. This means that clinical teams MUST screen every patient's NHS number against a national opt out list at NHS Digital prior to ANY data being entered onto the SSNAP webtool.

Your rights as a stroke patient

As a stroke patient with information about your care collected by SSNAP, you have rights to the following:

Access your data, request a copy of your data in standard format and/or update your information
You have the right to request a copy of the information we hold about you and to have any inaccuracies in your information corrected. For more information on how to access the data collected about you, please contact your hospital directly, as SSNAP does not hold patient identifiable information.

Restricting the use of your data, stopping your data being used, and/or deleting your data
Patients can choose to opt-out of the audit, such that their personal identifiable information will not be stored or used for any purpose by the audit. Opting out from SSNAP will not affect the care a patient receives. For more information on how to opt-out from the audit or access the data collected about you, please contact your hospital directly, as SSNAP does not hold patient identifiable information.

A full list of NHS trusts in England and Wales is available by following the links below:
https://www.nhs.uk/servicedirectories/pages/nhstrustlisting.aspx and
http://www.wales.nhs.uk/ourservices/directory/localhealthboards

To safeguard your rights, we will use the minimum personally-identifiable information possible.

Where we use automated decision making and how it affects you

Automated decision making is not used by SSNAP so patient data is not impacted in this way.

Who makes the decisions about using your data, if not the KCL

Only KCL, and HQIP as the data controller, make decisions about using your data.

Who to contact at the KCL to complain

As a patient you have the right to complain about the use of your data by SSNAP. Should you have any concerns or queries about any of the above please contact either the KCL data protection officer info-compliance@kcl.ac.uk or the HQIP data protection officer data.protection@hqip.org.uk. If you are not satisfied with the service provided by KCL you have the right to complain to the Information Commissioners Office (ICO) https://ico.org.uk/concerns/ or call their helpline on 0303 123 1113.

Additional information and resources

There is a wealth of information regarding the legal basis for collecting and using patient data by SSNAP. This is accessible on the patient and carer page on the SSNAP website:
https://www.strokeaudit.org/PatientInfo.aspx.

If you have any further questions or queries that are not addressed in these documents please contact the SSNAP helpdesk ssnap@kcl.ac.uk.