Accessing National Clinical Audit and Patient Outcomes Programme (NCAPOP) data: Guidance for applicants and data providers

Contents

I. Introduction 2

II. Legislation 2

III. Data controllers and data processors 3

IV. The role of the Healthcare Quality Improvement Partnership (HQIP) 3

V. The role of the applicant 4

VI. The role of the data provider 5

VII. The Data Access Request Group (DARG) 6

VIII. The Data Access Review Process 7

IX. Completing the Data Access Request Form (DARF) 8

X. Sharing unpublished NCAPOP data 20

XI. Data Breach 20

XII. Transparency 21

I. Introduction

1.1. The purpose of this document is to outline the process of applying for access to HQIP commissioned data sets including data collected as part of the National Clinical Audit and Patient Outcomes Programme (NCAPOP)

1.2. The guidance below should be reviewed in parallel and is intended to complement the HQIP Data Access Request Form (DARF), Data Sharing Agreement (DSA) and information listed on the HQIP website.

1.3. This guidance should be used by data access applicants during the process of making an application

1.4. This guidance should also be used by NCAPOP audit and clinical outcome review programme providers who are required to review, and where appropriate support requests for access to the data that they collect under contract to HQIP

1.5. Please note that although the guidance set out in this document is aligned with current information governance standards, it does not replace, supersede, or otherwise invalidate other available guidance and best practice

II. Legislation

2.1. The Data Protection Act 1998 (DPA) is an Act of Parliament of the United Kingdom of Great Britain and Northern Ireland which defines UK law on the processing of data about identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK. The DPA is complemented by the law of informational privacy which encompasses the common law of confidentiality and the right to privacy under the Human Rights Act 1998

2.2. The DPA sets out the position of the key roles involved in processing personal data: data controllers and data processors. Access to data must be authorised by the data controller who in law is the person or organisation which determines the purposes and manner in which the data is processed, and is responsible for that processing

2.3. Key definitions of the Data Protection Act are available on the Information Commissioner's Office (ICO) at https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

2.4. The Data Protection Act does not apply to the disclosure of patient data for deceased individuals. However, the General Medical Council (GMC) and other professional guidance explicitly states that a duty of confidentiality should still be maintained even after the patient is deceased. See GMC website: http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality_70_72_disclosure_after_patient_death.asp

2.5. For an overview of data sharing good practice please refer to the Information Commissioners Office Data Sharing Code of Practice, May 2011 https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

III. Data controllers and data processors

3.1. A data controller is either a person or an organisation who determines the purposes and the manner in which any personal data are, or are to be, processed

3.2. There can be more than one data controller for a dataset. In such circumstances, both parties would either be joint data controllers or data controllers in common

3.3. Joint data controllers occur when two or more persons or organisations act together to decide the purpose and manner of any data processing. NHS England, the Welsh Government and HQIP are therefore joint data controllers for personal data collected as part of the NCAPOP Programme

3.4. Joint data controllers must together agree all new purposes for the processing of the data

3.5. Data controllers in common occur when two or more persons or organisations share a pool of personal data that they process independently of each other for different purposes.

3.6. A data processor is any individual or organisation (other than an employee of the data controller) who processes the data on behalf and at the behest of the data controller. The NCAPOP audit providers are data processors on behalf of HQIP. Security requirements placed on data controllers in respect of processing on their behalf are set out in Part II of Schedule 1 of the DPA

3.7. When a request for access to data is approved by HQIP and data is shared with an applicant, that applicant will not become a data processor for the data that they receive as they will not be processing data on behalf of HQIP. They will become data controllers in Common with HQIP for this dataset

3.8. Where an applicant wishes to link a dataset for which it is a data controller in common with HQIP, to a separate dataset for which HQIP is not the data controller, and HQIP approves, the applicant will become the sole data controller for that new dataset unless specifically agreed otherwise

3.9. The ICO have created a guidance document '*data controllers and data processors: what the difference is and what the governance implications are'* which is available at: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

3.10. The ICO has a range of powers which it can bring to bear if an organisation fails to adhere to the DPA for a dataset for which it is the data controller. Further information is available on the ICO website: https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/. Please also see Section X of this guidance regarding Data Breach

IV. The role of the Healthcare Quality Improvement Partnership (HQIP)

4.1. The Healthcare Quality Improvement Partnership (HQIP) commissions and manages the National Clinical Audit and Patient Outcomes Programme (NCAPOP) on behalf of NHS

England (NHS E) and frequently the Welsh Government (WG). As such, HQIP is "joint data controller" with these organisations and is responsible for all data that are collected and shared as part of NCAPOP

4.2. Several NCAPOP projects have also been funded by the Scottish Government and other devolved administrations or Crown Dependencies with which HQIP similarly acts as Joint data controller

4.3. HQIP enacts its data controller responsibilities through its Data Access Request Group (DARG) which has representation from NHSE and the WG

4.4. The broad aim of the NCAPOP programme is to support clinicians to measure and improve the care they deliver, and enable patients, healthcare commissioners and regulators to be informed about the quality and outcomes of a wide range of healthcare services. HQIP commissions supplier organisations to collect and analyse data, and report the key findings and recommendations for over forty different areas of healthcare. These supplier organisations are 'data providers' for the purpose of data sharing requests

4.5. In certain circumstances, HQIP acts as either a joint data controller or a data controller in Common with another organisation(s). For instance, where one of the NCAPOP Programmes (for which HQIP is the data controller) links data with Hospital Episode Statistics (HES) or Office for National Statistics (ONS) Data (for which the NHS Digital is data controller), HQIP and NHS Digital become joint data controllers for the linked dataset

4.6. In order to meet its aim of improving the quality of clinical service and patient outcomes, HQIP has an obligation to support appropriate access to the data collected as part of NCAPOP. HQIP supports the sharing of NCAPOP data for the purpose of quality improvement, including research, service evaluation, and audit

4.7. Where DARG approve access requests, HQIP will:

- instruct the data provider to share the specified data items with the applicant, and
- remain data controller in common for the shared data in the form in which they are shared

4.8. HQIP will mediate in any dispute between the applicant and data provider. Where a data provider does not support an application, the applicant should inform DARG who will review the request alongside comments from both parties

4.9. HQIP reserves the right to request further information and visit any organisation housing data for which HQIP is data controller to ensure that the information provided in the application is accurate and being processed as stated in the application. If, upon inspection, the processing of the data is not consistent with the information provided in the application upon which HQIP approval was granted, HQIP may revoke the approval. In this instance, all data must be securely destroyed. No publications or other outputs from the applicant or their host organisation will be allowed to use or report these data in any form.

V. The role of the applicant

5.1. "The applicant" is the organisation making the data access request. It is expected that the applicant will host the data once received unless stated otherwise

5.2. It is expected that the applicant will discuss their request in detail with the data provider in the first instance and prior to submitting an application to HQIP. The data processor in many cases will be well placed to advise the applicant on considerations around information governance, clinical relevance and methodology

5.3. DARG will take into consideration the view of the data provider when considering an application. The applicant is therefore expected to work closely with the data provider to ensure that the application is appropriately considered and detailed, and where possible, is supported by the data provider. Applications which have not been discussed with and reviewed by the data provider will not be considered by DARG

5.4. An appropriate signatory from the applicant should sign the data access request form having first read and understood the information contained within this guidance and the terms and conditions of the data sharing agreement. The signatory must be able to accept liability on behalf of the applicant organisation for any misuse of the data

5.5. Once an application is approved by the DARG, the applicant must comply with the terms and conditions of the DSA for the duration of the period during which they hold the data. Please also see relevant information in section IX of this guidance relating to the Data Sharing Agreement

5.6. Once an applicant receives data as part of a data access request, it becomes a data controller in Common with HQIP

5.7. Once an application has been approved by DARG and the data transferred, applicants should submit an amendment to their application if they wish to make any changes to the scope of the application, personnel accessing the data, the data items or other changes.

5.8. If the applicant learns that information detailed within the application is no longer accurate during the period which the applicant is authorised to process the data, the applicant must inform HQIP, as the data controller within one week of the change being identified. The nature of the change may affect the DARG approval

5.9. Applicants cannot have intellectual property rights over personal data but can have rights over the methodology they apply to personal data and data derived from that personal data provided it is anonymised to the standard required by ISB Anonymisation Standard for Publishing Health and Social Care Data. Any such intellectual property rights associated with the data prior to processing by the applicant remain vested solely in HQIP

5.10. If any data breach occurs concerning data for which HQIP is data controller in common with an applicant, the applicant should inform HQIP immediately upon discovery of the breach. Please also see Section XI Data Breach

VI. The role of the data provider

6.1. The "data provider" is the organisation which releases the data to the applicant, once the DARG has granted approval for the application

6.2. The data providers for the purposes of this application process will be the organisation(s) processing data on HQIP's behalf and under contract to HQIP. Normally they will be suppliers of National Clinical Audits and the Clinical Outcome Review Programmes which form the NCAPOP

6.3. NCAPOP data providers are required to support the release of data for secondary uses and incorporate the principles and practices outlined within this guidance into their data sharing protocols

6.4. The data provider is expected to advise the applicant on the data items that they hold which are available for access and the form in which they can be shared prior to the application being submitted

6.5. DARG will take into consideration the view of the data provider when considering an application, given their expertise of the clinical area and knowledge of the data. Where the data provider supports an application, the clinical lead or the chair of an appropriate scientific committee, and an appropriate signatory from the organisation which holds the contract with HQIP will be required to sign the Data Access Request Form (DARF)

6.6. Where the data provider does not support an application, the data provider should write to HQIP setting out their concerns. The application will then be considered by DARG in light of the data provider concerns

6.7. The data provider can charge a cost recovery fee for works undertaken to support and release NCAPOP data.

6.8. Once support has been granted by DARG, the data provider will share a copy of the data in a timely manner as agreed between the applicant and provider

6.9. Where an applicant wishes to utilise HQIP data to contact a cohort of patients the data provider may be required to initially contact that cohort before the data can be released to the applicant

6.10. HQIP support the principle of NCAPOP projects establishing or co-opting appropriate panels or committees to internally review applications prior to their sign-off and submission to DARG. Any such panel would usually include clinical and methodological input

6.11. HQIP support the principle of NCAPOP data providers applying an appropriate cost recovery model to cover the resource expended in preparing and transferring the data

6.12. HQIP would expect that data providers release data within a reasonable time following DARG approval. HQIP accepts that the timeframe may vary depending upon the complexity of the data requested, the number of data access requests being processed and the scope of core audit or clinical outcome review programme activity being undertaken at that time. HQIP would expect data to be released within a number of weeks where possible.

VII. The Data Access Request Group (DARG)

7.1. HQIP's DARG meet on a monthly basis to review requests for access to NCAPOP data. It is authorised to approve requests on behalf of HQIP, NHS E and the Welsh Government and provides these parties with assurance that the requests are processed in line with the DPA

7.2. DARG is comprised of senior members of HQIP, as well representatives of NHS England and the Welsh Government. These members review applications as joint data controllers and have access to expert methodological advice

7.3. The DARG terms of reference (including membership) and meeting dates are listed on the HQIP website

VIII. The Data Access Review Process

8.1. All completed applications should be submitted to HQIP's datasharing@hqip.org.uk inbox using HQIP's Data Access Request Form (DARF). Applications on any other form or application will not be accepted

8.2. Applications can either be submitted by the applicant, or by the data provider on behalf of the applicant

8.3. HQIP will confirm receipt of the DARF and undertake the initial review of each application within five working days

8.4. Each application will be allocated a reference number by HQIP. This reference number should be used on all correspondence relating to the application

8.5. DARG require all relevant sections of the DARF to be completed in full and all relevant supporting information and signatures garnered prior to submission. Incomplete forms will be returned to the applicant.

8.6. Where DARG require information detailed within a DARF to be clarified, the clarifications will be communicated to the applicant within seven days of a DARG meeting

8.7. DARG will take into consideration the views of the data provider when reviewing each application given their expertise (see section 6.6)

8.8. DARG review each application against the following criteria:

- is the proposed use of the data clinically appropriate?
- is the proposed use of the data methodologically sound? This includes considerations around whether the requested data is sufficient and appropriate to answer the research question (e.g. have appropriate casemix variables been requested/is patient-level data necessary or can publically available aggregate data be used to minimise requirements)
- Does the applicant have the necessary legal permissions, information governance policies and security arrangements in place for them to receive, use and manage the data securely and appropriately?

8.9. Where DARG requires specialist input, it will refer the application to HQIP's Information Governance Advisory Group (IGAG) for review. The applicant will be informed of this referral if there is likely to be any resultant delays

8.10. DARG will seek to discuss applications which are submitted prior to the submission deadline and that do not require clarifications, at the following DARG meeting. However, during times of high demand, it may be necessary for applications to carried over to the following meeting

8.11. DARG meetings, submission and outcome dates are listed on the HQIP website

8.12. In instances where DARG has requested information about an application and no response has been received within sixty days of the communication, the application will be closed and the applicant will be required to reapply

IX. Completing the Data Access Request Form (DARF)

To apply for access to NCAPOP data, applicants must complete a Data Access Request Form. This section provides guidance as to how to complete the DARF and why the information is required by DARG. All sections of the DARF must be completed unless stated otherwise.

Applicants wishing to reproduce tables, text or other information that is included in an NCAPOP project report or output under HQIP copyright should contact HQIP separately at datasharing@hqip.org.uk.

Section 1 - Applicant Information

- The applicant should specify the title that has been attributed to the project. This should be the same as the title that has been used to describe the project on any associated requests or applications, or should be the title that best describes the project

- The application should be completed by an employee of the organisation that will be receiving the data. Where more than one organisation will receive the data, one organisation should act as the primary applicant and complete all relevant sections of this form. Where necessary, all other organisations receiving the data should complete Appendix 1 of the DARF

- The address of the applicant organisation and contact details for a primary contact within that organisation should be listed. Any queries about the application will be addressed to the primary contact listed

- The applicant should check which organisation type best describes the applicant organisation: NHS Healthcare Provider; Academic Institution; Healthcare Regulator; Other Healthcare Body; Local Authority; Individual Citizen; Commercial Body

- Where 'Individual Citizen' is checked as the organisation type, it is understood that an individual or group of individuals are applying for the data outside of their formal role at any particular organisation. It is therefore understood that any data received will be stored and accessed from a private system and not that of any of their employers

- Over forty projects comprise the NCAPOP programme. Applicants should detail which NCAPOP project(s) they wish to access the data for. For reference, a list of NCAPOP projects and their Project Managers are listed on the HQIP website

Section 2 - Application Type

- Applications must state whether their application represents a new request for data, or whether it is an: extension; renewal; or amendment to a previous application.

- An 'Extension' is a request to extend the retention period for data that has previously been approved by DARG

- A 'Renewal' is a request for additional data of the same type that has been collected by the data provider since the application was approved by DARG

- An 'Amendment' is a request to change the scope, data fields required, personnel accessing the data, or any other change to an application previously approved by DARG

- Where the application is not a new request, the applicant should detail the application reference number for the previously approved request, along with the date that had previously been listed as the end of the retention period for the data

- In such circumstances, the applicant should summarise the change(s) to their previous application and populate the information listed from their previous form. The applicant will be required to provide updated signatures

Section 3 - Project Type

- Applicants should state whether their project type can best be described as: Research; Service Evaluation; or Clinical Audit, or provide an alternative

- The Health Research Authority (HRA) has developed a self-assessment tool to provide guidance as to whether a project constitutes research. This is available at http://www.hra-decisiontools.org.uk/research/

- Applicants requesting patient level data for the purpose of research should consider whether ethics approval is required. The HRA, provides guidance on how to determine whether or not ethics approval is required at: http://www.hra.nhs.uk/documents/2013/09/defining-research.pdf

- The HRA website provides a flowchart of the steps required to apply for Research Ethics Committee (REC) approval at http://www.hra.nhs.uk/resources/applying-to-recs/nhs-rec-application-process-flowchart/

- Whilst applications for data can be discussed with HQIP prior to confirmation of relevant approvals being received, all approvals, including research ethics and Section 251 of the NHS Health and Social Care Act 2006 (S251), will need to be in place before DARG will formerly review and approve an application

- For research projects, where ethics approval has been granted, a copy of the confirmation letter should be submitted along with the application. Where ethics approval is not required,

the applicant should submit confirmation from the HRA decision tool that ethics approval is not required

Section 4 - Project Details

- DARG will only authorise the release of data for a clinically appropriate purpose, and where the methodology underpinning any analysis of the data is felt to be sound

- Applicants are required to detail the objective and rationale behind the project, and the methodology that will be used, as described in a project protocol. Applicants should provide as much detail as possible to support DARG in their understanding of the request

- Applicants are required to list the proposed completion date of the project. This is defined by the latest project-specific activity, excluding final destruction of the data

Section 5 - Outputs and Publications

- NCAPOP is delivered using public funding, through a mixture of NHS and centrally funded resource. HQIP is therefore committed to ensuring that, where possible, all data, outputs and publications are made publically available for the benefit of the public and the NHS

- All NCAPOP projects are required to publish their findings widely and make their reported data available on data.gov and increasingly on NHS Choices and MyNHS. Applicants for data, especially for the purposes of research, are therefore expected to publish any findings or outputs resulting from their analysis of NCAPOP data, as agreed within the application

- As part of the application, applicants should detail each intended output or publication resulting from the project, and describe the level of granularity of data that will be made available within that output. The granularity of the data requested should be proportionate to analyses planned and the level of publication intended

- All outputs must be appropriately anonymised to minimise the risk of re-identification of patients. The applicant should therefore confirm that that all publications or outputs will be anonymised to the level required by the ISB Anonymisation Standard for Publishing Health and Social Care Data

- Applicants should provide copies of all publications and / or outputs resulting from NCAPOP data to both the data provider and to HQIP for information, referencing the application number

- As part of any output or publication, applicants should reference that the data used *"was collected on behalf of the Healthcare Quality Improvement Partnership (HQIP) by (xxx provider) as part of the National Clinical Audit and Patient Outcomes Programme"*

Section 6 - Project Funding

- DARG will review applications from commercial parties, or that have a commercial interest, on a case by case basis to determine whether the merits of the project can be supported

- Where a commercial organisation has had input into, or will form part of the project team, the name of the organisation should be listed as well as the nature of the association

- Where dedicated funding has been secured from outside the applicant organisation, the name of the organisation(s) providing funding, the "funding body(s)", should be listed and an appropriate declaration of interest made (see section 7)

Section 7 - Declaration of Interest

- Declarations of interest from all applicants are required. If none, please state none.
- DARG will review this detail and consider whether there is a potential conflict of interest on the basis of the declarations made
- A conflict of interest for the purposes of this process is defined as a situation in which a person has a private or personal interest sufficient to appear to influence the objective exercise of his or her official duties as, say, a public official, an employee, or a professional
- If a member of the applicant project team is also a member of the data provider, this should be declared from the outset, and description of the appropriate mitigations applied provided (eg. the data provider arranges non-conflicted peer review of the merits and methodology of the application)
- DARG will review such applications on a case by case basis to determine whether the application can be supported

Section 8 - Data Summary

- The majority of NCAPOP projects collect data from healthcare providers in England and Wales. Some also collect data from other devolved administrations and Crown Dependencies. These arrangements will be different for each NCAPOP project

- An applicant should discuss the geographical coverage of the data available with the data provider and then detail within the application the geographical coverage of the data they are requesting. Coverage is defined as the location of the healthcare services who originated / initially provided the extract of data you are requesting

- To enable DARG and the data provider to properly understand the parameters of the data requested, each applicant must describe fully the inclusion and exclusion criteria for the data extract that they are requesting and how the cohort is defined (diagnosis, treatment, follow-up etc). An example of a description of a cohort would be: *all patients diagnosed between 1st January 2014 – 31st December 2014 with latest clinical event data 6 months after diagnosis.* However details of which pathologies, treatments and outcomes are included would also need to be provided

- Whilst the majority of data access requests are for data that has already been collected, DARG can consider requests which include provision for periodic future updates or refreshes of data during specific points during the lifecycle of the applicant's project. The applicant would need to describe the frequency and dates of the required refreshes and the reason why they are required

- NCAPOP projects routinely link the data that they collect to other external datasets for the purposes of the project. For those linked data only, HQIP is the joint data controller with the data controller for the dataset to which the NCAPOP data has been linked

- HQIP's DARG can only independently authorise the release of data for which it is the sole data controller. Applicants are advised to apply for unlinked Audit / unlinked Clinical Outcome Review Programme data where possible

- HQIP works closely with other data controllers, such as NHS Digital, to facilitate the sharing of linked audit data. Applicants wishing to receive linked audit data should contact HQIP at datasharing@hqip.org.uk before completing the DARF for advice

Section 9 - Data Type

- For the purposes of data access, HQIP recognises three types of data: anonymised; limited access de-identified; and personal data

- DARG accepts that with the sharing of data there will always be a risk of re-identification. DARG therefore requires that all reasonable steps are taken to avoid re-identification of individuals during the handling and reporting of data

- Where possible, data should be anonymised as far as is practicable before sharing

Anonymised Data

- The guiding principle behind anonymisation is to avoid the identification of any individual using one or more linked items of data

- A wide variety of de-identification techniques exist, including, but not limited to aggregation, suppression, sampling and generalisation

- There are two standards of anonymisation; for general publication and for access by a limited number of approved people for a defined purpose. All data shared with applicants should be de-identified to the extent possible even if anonymisation to neither standard can be achieved

- HQIP considers a dataset to be anonymous for the purposes of publication if it complies with the Information Standards Board Anonymisation Standard for Publishing Health and Social Care Data

- Sharing data that are not personal, e.g. aggregate statistics that cannot identify any individual are not subject to the DPA or the law of informational privacy. However, HQIP requires applications for all data requests to be submitted to the DARG to ensure that they, as data controllers, can keep a contemporaneous log of all data sharing involving NCAPOP data

- Where anonymised data is requested, applicants will not be required to complete sections 13-18 of the DARF. In such cases, the data provider must provide assurance that their process of anonymisation is compliant with the ISB Anonymisation Standard and the ICO's Anonymisation Code of Practice

Limited Access De-identified Data

- Where the purpose behind a request for data cannot be supported by anonymised data alone, the sharing of data that has been de-identified to the standard required for limited access disclosure by the ICO in section 7 of its Anonymisation Code of Practice: see https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/ can be authorised
- At the time of publication of this guidance there is no agreed uniform definition of limited access de-identified data. For the purpose of data access, HQIP defines limited access de-identified data as data that has been de-identified but has not been fully anonymised in line with the Information Standards Board Anonymisation Standard for Publishing Health and Social Care Data. Although reasonable steps have been taken to minimise the possibility of re-identification a risk remains, therefore access to the data has been restricted to named individuals, under certain conditions and for a defined purpose as agreed within the DARF application and subsequent DSA

- Limited access disclosure therefore allows for the disclosure of 'richer data' than can be achieved by the anonymisation process listed above

- It relies upon robust governance arrangements to be in place to minimise the risk of re-identification; see the ICO's Anonymisation: managing data protection risk code of practice summary

- Pseudonymisation, whereby the identity of individuals is retained by data providers but withheld from applicants, is a form of limited access disclosure

Personal Data

- 'Data' is recorded information. 'Personal data' is data that relates to an individual who can be identified from it, or from it and other information a recipient has or is likely to have[1]

- Under the Data Protection Act 'personal data' is data about living people, but for the purposes of this guide 'personal data' includes information about identifiable dead people. Confidential information remains confidential after death, and relatives are in any event owed an ethical duty[2]

- All organisations which hold, manage or process personal data must comply with information governance procedures, practices and legislation

- Personal data that are shared, are subject to the Data Protection Act (DPA) and associated codes of practice (please also refer to the Information Commissioners Office (ICO), Data Sharing Code of Practice, May 2011, https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf)

- Personal data related to health are likely to be private and confidential under the law of informational privacy. It is safer and easier to treat all health personal information as private and confidential. There has to be a legal basis for using or disclosing it

- HQIP needs to assure itself at all times that an appropriate legal basis exists to support all of the flows of confidential personal information for which it is data controller

[1] Data Protection Act 1998 section 1. The Act refers to 'data controller' but 'recipient' better reflects reality.

[2] *A guide to confidentiality in health and social care: references*, NHS Digital (formerly HSCIC), 2013, page 8

- In order for a flow of personal data to take place lawfully, the organisation transferring the data must have a legal basis to transfer the data for the specified purpose, and the organisation receiving the data must also have a legal basis to receive the data for that specified purpose

- Similarly, for an organisation to act upon or link personal data, that organisation must first have an appropriate legal basis

- The two most common forms of legal permission covering personal data are:
    - Written, informed patient consent
    - Permission to collect patient identifiable data without individual patient consent under S251 of the NHS Health and Social Care Act 2006

- Other legal permissions exist, such as Directions under Section 254 of the Health and Social Care Act (2012)

- Many of the NCAPOP projects do not currently use a consent model to collect data. Those that hold personal data under S251 may not have permissions to share personal data for the purposes of research, or for the purpose detailed within a specific data access request. As such, any applicant requesting personal data should first discuss with the data provider whether appropriate permissions exist to support the sharing of personal data for the purposes detailed within their application

- DARG will therefore only consider requests for personal data where all of the following are met:
    - The project purpose cannot be met with either anonymised or limited access de-identified data
    - The NCAPOP project has a legal basis to share personal data for the purposes listed within the application
    - The applicant has a legal basis to receive and act upon personal data for the purposes of their application

Section 10 - Data Fields

- Data, even anonymised data, should only be shared if it is necessary to address the purpose outlined within the project scope. DARG will not approve applications where more variables are requested than are explicitly required to support the stated aims and objectives of the project

- In order to understand the data that is being requested, DARG require applicants to submit a table of all data items that they require to meet the stated aims and objectives of the project

- Data providers are expected to provide a table of data items collected as part of the NCAPOP project to applicants to support them with their application. On this table, the data provider should list which data items form part of the HQIP-controlled dataset and which data items (if any) are sourced from other data controllers such as HES / ONS data

- Data providers should detail whether any restrictions or suppressions apply to any data items that they hold

- Applicants should discuss with the data provider what data items and in what format the data provider(s) are legally allowed to share, prior to submitting an application to DARG

- DARG will review the data items requested against the description of the project and may query why specific items have been requested if the relationship between the two is unclear. Applicants are encouraged to consider including justifications against specific data fields to support DARG's understanding of the application. This will minimise the potential for delays

Section 11 - Data Flows

- DARG will need to understand which organisations (if more than one) will be receiving the data and in what format (anonymised / limited access de-identified / personal). To support this understanding, applicants are asked to graphically illustrate:

    - All locations where the data will be housed/stored
    - All transfers of data that will take place between organisations (and premises if an organisation has more than one premises where the data will be housed/stored)
    - The format of the data as part of each transfer (anonymised (including suppressed aggregate), limited access de-identified (including pseudonymised), personal / identifiable)
    - If applicable, where the data will undergo any linkages to other datasets

- A sample dataflow map is included as Appendix 1 of this document

Section 12 - Project Team employed by Applicant Organisation

- To understand who will have access to the requested data, all members of the project team who are employed by the applicant organisation should be listed.

- In Section 21, the applicant organisation is required to confirm that all members of the project team will abide by the terms and conditions detailed within the HQIP Data Sharing Agreement (DSA). The applicant must confirm that the individuals listed within this section each have a formal contract with the applicant organisation

- Where the data flow map in Section 11 details the transfer of data that has not been anonymised in line with the ISB Anonymisation Standard, to additional organisation(s) who will process data as part of the applicant's project, those organisation(s) should complete Appendix 1 of the DARF application

Section 13 Data Protection

- The Data Protection Act 1998 requires every organisation that processes personal data to register with the Information Commissioner's Office (ICO), via the ICO website. The ICO also provides a useful guide to data protection

- Applicants requesting personal data must detail the registered name, registration number, dates of the ICO registration period, and the purpose for which the applicant is registered to process personal data. Details of each organisation registered with the ICO website are available at https://ico.org.uk/esdwebpages/search

- The regulations governing the transfer of personal data are aligned across EU/EEA countries. Until December 2015, the transfer of personal data outside of the UK, but within the EU (European Union) or European Economic Area (EEA), were covered under the Directive 95/46/EC ("the Directive")[3]. The legislation has since been updated and a FAQ sheet is available at: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

- Where an applicant wishes to share personal data outside of the EU or EEA areas, the applicant should refer to the FAQs on the http://ec.europa.eu/justice/data-protection/international-transfers/files/international_transfers_faq.pdf and specifically state how the recipient organisation is in compliance with the Eighth Data Protection Principle

Section 14 - Legal Basis

- All organisations which hold, manage or process personal data must comply with the DPA

- HQIP needs to assure itself at all times that appropriate legal bases exist to support all flows of personal data for which it is data controller

- An applicant requesting personal data must first have a legal basis to receive it. The two most common forms of legal basis are:

    - Written, informed patient consent (informed consent is agreement to a specific course of action, in this case the use of personal information about them for the research purpose, that is freely given by a patient with mental capacity)
    - Permission to collect patient identifiable data without individual patient consent under S251 of the NHS Health and Social Care Act 2006

- Where a legal basis does exist, applicants should detail what the legal basis is for them to receive and use personal data. Where the permissions centre around written, informed patient consent, the applicant should attach a copy of the consent form as part of the application. Where the permissions centre on S251 approval, the applicant should attach both the application form and approval letter as part of the application

- If an applicant holds a separate legal basis that is not consent or S251, they should provide full details

- Where Personal data is requested, DARG will only review and approve applications which can evidence an appropriate legal basis. However, to minimise potential delays, HQIP will review and advise applicants about their applications **prior** to receipt of an appropriate legal basis and formal submission to DARG

- Applications for S251 approval are reviewed by the Confidentiality Advisory Group. Further information on S251 is available on the Health Research Authority website

Section 15 - Fair Processing

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31 et seq.)

- One of the principles of the DPA centres on fair processing. This requires reasonable steps to be taken to inform people to enable the use of their information to be fair to them: see https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/

Section 16 - Information Governance (Including Security)

- All Health and Social Care service providers, commissioners and suppliers as well as organisations that have access to personal data must ensure that they have appropriate systems in place to manage data effectively. This includes the storage, transfer, access to and linkage of the data. They must also have appropriate security measures in place to meet the requirement set out in the Data Protection Act

- Where data is transferred from one organisation to another, it is the responsibility of the data controller to assure themselves that the recipient organisation similarly has appropriate management and security systems in place. DARG cannot authorise the release of personal or limited access de-identified data until it has been assured that the applicant has such systems in place

- The IG Toolkit is a self-assessment tool commissioned by the Department of Health (DH) and developed and maintained by NHS Digital to enable organisations to assess and evidence their compliance against information governance requirements

- As part of an application, each organisation transferring, accessing, operating on, or linking data that has not been adequately anonymised in accordance with the ISB Anonymisation Standard must evidence as part of their application that they are IG Toolkit compliant to Level 2 by attaching a printout of their IG Toolkit score, or confirm what technical and organisational measures will be taken to prevent unauthorised or unlawful processing of the data, accidental loss, destruction, or damage to it. They should also demonstrate how the processes and procedures within their organisation align with the requirements of the IG Toolkit

- All NCAPOP data providers are IG Toolkit compliant to Level 2 or above

- Further information about the IG Toolkit is available online at: https://www.igt.hscic.gov.uk/resources/About%20the%20IG%20Toolkit.pdf

Section 17 - Retention and Destruction

- The date that the organisation will continue to house the data, the 'retention period', should be specified within the DARF. Personal or limited data should only be retained for the duration of the project and should mirror the proposed completion date listed in Section 4 of the DARF unless a there is an essential reason for its retention beyond this period, or it is subject to a retention period, in particular under the Department of Health's retention schedule: see http://www.nhs.uk/chq/Pages/1889.aspx?CategoryID=68

- Where an applicant is reliant upon the renewal of specific permissions to maintain or act on the data, such as the renewal of CAG approval to provide a legal basis under S251, these renewals and the associated dates must be specified within the application form

- It is the responsibility of the applicant to initiate the submission of an extension to their application to DARG in a timely manner. Where such approvals lapse (i.e the date parameter

for holding or processing data has expired) the applicant is expected to destroy the data in line with section 17 of the DARF and submit a certificate of destruction to HQIP using Appendix 2 of this guidance within two weeks of destruction of the data.

- Where the legal basis to hold and access personal data has lapsed without an extension application having been submitted, the applicant must destroy the data immediately and submit a certificate of destruction to HQIP using Appendix 2 of this guidance within two weeks of destruction of the data

- The method of destruction of the data at the end of the retention period should be considered and clearly articulated within the DARF

- Once the retention period for the data specified within the application expires, the applicant must securely destroy the data in line with the method articulated within the application, and complete and return the certificate of destruction (Appendix 2 of this guidance) to HQIP. Please note that it is the responsibility of the applicant to initiate an extension or confirm that the data has been destroyed

- If the applicant intends to retain the data beyond the end of the stated retention period, they should apply to DARG at least two months prior to this date

Section 18 - Intention to Link Data

- Where an applicant intends to link a dataset received as part of this application, they should detail which dataset they intend to link the data to, which organisation will undertake the linkage, and how the linkage will be performed

- If a third party will conduct the linkage, the applicant should ensure that an appropriate legal basis is in place to transfer the data to the third party, and that the third party has an appropriate legal basis to receive the data and act upon it for this specific purpose. All relevant information must be included in this application

- If an organisation links two or more datasets together that have not previously been linked, they will become the sole data controller for this new dataset

Section 19 - Further Disclosure

- To minimise the risk of re-identification of any individuals, applicants are required to confirm that data that has not been anonymised in line with the ISB Anonymisation Standard will **not** be disclosed to anyone who has not been listed within this application

- If at a later date the applicant would like to include other individuals as part of the project team, they must submit an amendment request to the approved application before proceeding

Section 20 - Further Information

- Applicants are encouraged to include any additional information that may support their request in this section

Section 21 - Data Sharing Agreement (DSA)

- The DSA sets out the framework for the sharing of data by HQIP. The terms and conditions detailed within the DSA reflect best practice in information governance and are based upon current guidance and legislation

- The DSA is an agreement between HQIP as data controller, the data provider, and the applicant(s) which defines the principles and procedures that each party will adhere to, and the responsibilities each party owes in respect of the other

- All organisations that will receive data as part of the application that has not been anonymised in line with the ISB Anonymisation Standard are required to confirm that that they will abide by the terms and conditions detailed within the HQIP Data Sharing Agreement for the duration of the period that they hold the requested data

- The most recent version of the DSA is listed on the HQIP Website. The applicant(s) will remain bound by the terms and conditions of the version of the DSA detailed on their DARF

- If an applicant does not agree to abide by the terms and conditions detailed within the HQIP Data Sharing Agreement, DARG cannot approve the application

Section 22 - Attachments Checklist

- The Attachments checklist details the documents that should be enclosed with the application if the information has not been detailed within the application form

- Applicants are required to provide a detailed list of data items requested and a data flow map to support each application. Additional information will be required dependent on the nature of the application

Section 23 - Authorised Signatories

- A responsible officer with designated legal authority to enter into such an agreement on behalf of their organisation must sign the application form on behalf of the applicant **prior** to its submission to HQIP

- By signing the application form, the signatory agrees for their organisation to be bound by the terms and conditions detailed within the DSA. Where appropriate, this will usually be the principle/lead investigator or a member of the contracts office

- The clinical lead or chair of the audit or clinical outcome review programme scientific, or other appropriate committee must sign the DARF. A responsible officer from the data provider must also sign the DARF **prior** to its submission to HQIP

- If the data provider or the clinical lead / chair of an appropriate audit or clinical outcome review programme scientific committee do not feel that they can support the application, they should detail their reservations in writing to HQIP separately at the point of application submission to DARG. DARG will then consider this information in the context of the application

- Once the DARF has been completed and signed by the Applicant(s); Clinical Lead / chair of an appropriate scientific committee from the audit; and a responsible officer from the Data

Provider, it should be submitted along with any supporting information to datasharing@hqip.org.uk

- Authorisation to release the data requested will only be in place once HQIP sign the application form as data controllers

X. Sharing unpublished NCAPOP data

10.1. The purpose for which NCAPOP projects and their data flows have been established is to facilitate quality improvement in healthcare. The primary output resulting for the audit data is the National Audit or Clinical Outcome Review Programme report

10.2. DARG would not support a request for unpublished data that, through the timing of its outputs, may potentially undermine or diminish the impact of one of the NCAPOP publications

10.3. DARG will however, review requests from applicants for access to unpublished audit data in specific scenarios. These include, but are not limited to:

- Sharing data with funding bodies
- Presentation of data at conferences or meetings
- Sharing data with a project once the NCAPOP project data has been validated and confirmation has been received that the National Report will precede any output generated by the applicant

10.4. DARG will review such requests on a case by case basis and would seek the support of the data provider prior to approval

10.5. In circumstances where an applicant wishes to reproduce a specific table or other aggregated data which has already been published by the audit or clinical outcome review programme for the purpose of a presentation at a conference or meeting, it may not be necessary for the applicant to complete the full DARF. Applicants should contact HQIP directly at datasharing@hqip.org.uk to discuss their request

XI. Data Breach

11.1. A data breach is an incident whereby data is shared, processed, accessed, viewed, or stolen with or by parties who do not have permission to receive or act upon such data

11.2. As data controller HQIP is responsible for the management of all data collected as part of the NCAPOP programme

11.3. In the event of a breach or potential breach, HQIP may advise, or may itself be required, to inform other authorities, including but not limited to, the Information Commissioners Office (ICO)

11.4. If any data breach occurs, the applicant (who is either joint data controller or data controller in common with HQIP) must inform HQIP in writing **immediately upon discovery of the breach**

11.5. If the breach or potential breach was a result of negligence on the part of the applicant or their host organisation, HQIP reserves the right to withdraw the DARG approval. In this instance, all data will need to be returned to the audit from which the data were requested, and all copies securely destroyed. No publications or other outputs from the applicant or their host organisation will be allowed to use or report these data in any form

XII. Transparency

12.1. HQIP is committed to openness and transparency about how data collected as part of the NCAPOP programme is used, managed and transferred. NCAPOP providers are required to publish a full data flow diagram detailing which organisations hold data, in what format, and how it is transferred between them

12.2. HQIP will also publish details of all successful and non-successful applications for secondary use of the data on the HQIP website following DARG meetings

12.3. HQIP requires all NCAPOP providers to conform with the fair processing provisions of Schedule 1 Part I of the DPA and the guidance given by the ICO

Glossary

Confidentiality Advisory Group (CAG) – CAG is appointed by the Health Research Authority to provide advice on uses of data as set out in the legislation under two legal frameworks; The Health Service (Control of Patient Information) Regulations 2002 (also known as 'section 251 support') and The Care Act 2014. CAG review applications to process personal data under Section 251 of the NHS Health and Social Care Act 2006

Data Access Request Form (DARF) – The DARF is the application form which applicants requesting access to data from the NCAPOP programme will need to complete and submit to HQIP for review by DARG

Data Access Request Group (DARG) – DARG is the group responsible for reviewing and approving applications for access to data collected under contract to HQIP as part of the NCAPOP programme

Data.gov.uk – Data.gov.uk is a UK Government website which publishes non-personal UK government data

Data Protection Act (DPA) –The Data Protection Act 1998 is an Act of Parliament of the United Kingdom of Great Britain and Northern Ireland which defines UK law on the processing of data about identifiable living people

Data Sharing Agreement (DSA) - The DSA is an agreement signed by HQIP as data controller, the data provider, and the applicant(s) following approval of an application by DARG which defines the principles and procedures that each party will adhere to, and the responsibilities each party owes in respect of the other

Healthcare Quality Improvement Partnership (HQIP) - 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, and in particular to increase the impact that clinical audit has on healthcare quality in England and Wales. HQIP holds the contract to manage and develop the National Clinical Audit and Patient Outcomes Programme (NCAPOP), comprising more than 30 clinical audits that cover 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 audits, also funded by the Health Department of the Scottish Government, DHSSPS Northern Ireland and the Channel Islands

Health Research Authority (HRA) - The HRA is an organisation dedicated to protecting and promoting the interests of patients and the public in health and social care research

Information Commissioners Office (ICO) - The ICO is an independent body set up to uphold information rights in the public interest by promoting openness by public bodies and data privacy for individuals

Information Governance Advisory Group (IGAG) – A group which provides independent advice to HQIP on information governance issues

ISB Anonymisation Standard for Publishing Health and Social Care Data – The standard which outlines the agreed and standardised approach, grounded in the law, for distinguishing between identifying and non-identifying information. It specifies a set of standard tools for ensuring, as far as it is reasonably practicable to do so, that any information published (for example, as part of the transparency agenda) cannot identify individuals

My NHS - A website dedicated to publishing healthcare information primarily to those working within the NHS

National Clinical Audit and Patient Outcomes Programme (NCAPOP) – See Healthcare Quality Improvement Partnership (HQIP)

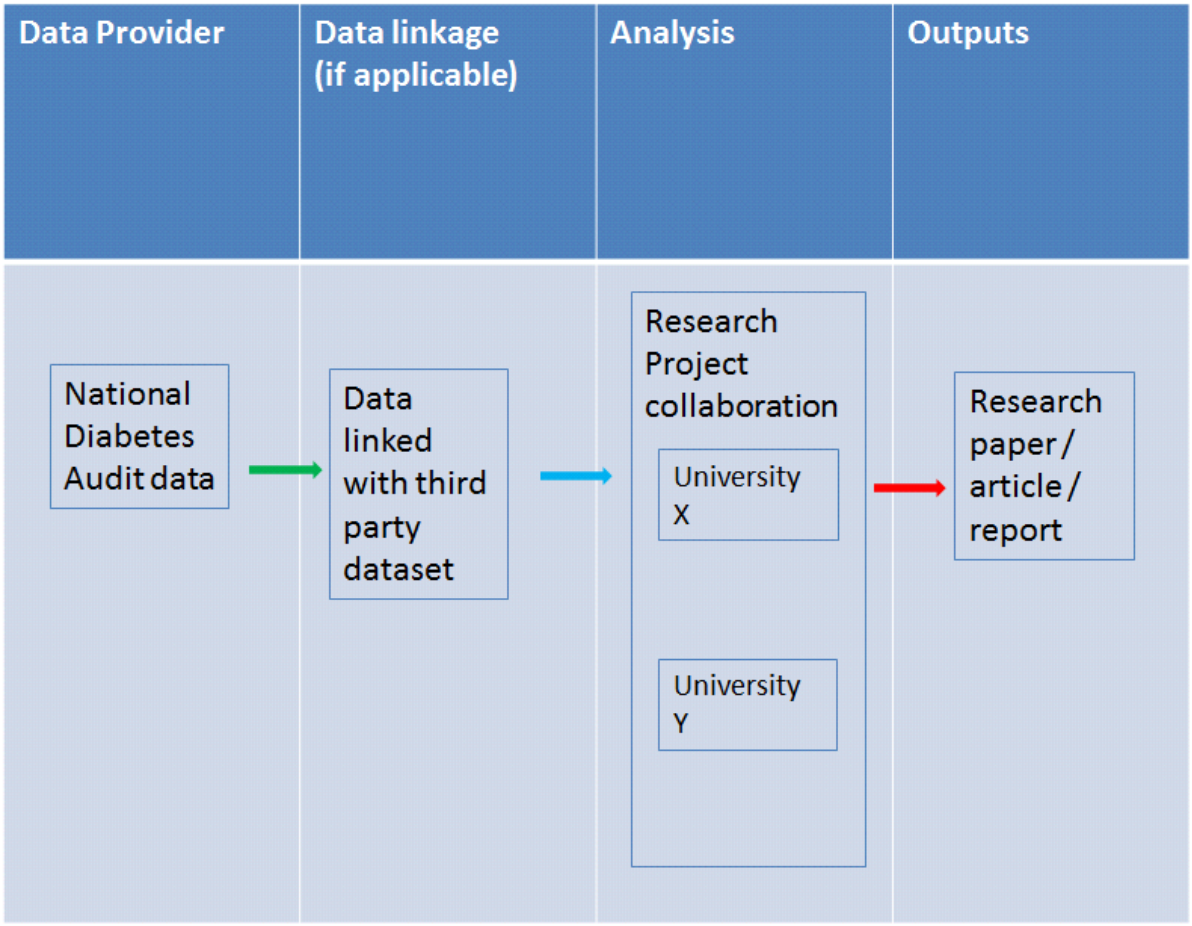
NHS Choices – A website dedicated to publishing healthcare information primarily to the public

NHS Digital – Formerly the Health and Social Care Information Centre, NHS Digital is the data controller for various datasets including, but not limited, to Hospital Episode Statistics (HES) and Office for National Statistics (ONS) data.

Section 251 of the NHS Health and Social Care Act 2006 (S251) – Section 60 of the Health and Social Care Act 2001 as re-enacted by Section 251 of the NHS Act 2006 allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purpose. Applications for S251 approval are reviewed by the Confidentiality Advisory Group (CAG)

Appendix 1: Example data flow diagram

Key:
Green= Personal data (S251)
Orange= Personal data (consented collection or other)
Blue= Limited access de-identified data
Red= Anonymised data
Italics= Future data linkage



Appendix 2: Certificate of destruction template

Certificate of Destruction	
In accordance with the Data Access Request Form and Data Sharing Agreement, this form must be completed by applicants at the end of their data retention period and a copy sent to HQIP	
Data Access Request reference number	
Organisation	
Method of destruction *Please detail the method used for destruction of the data*	
Date of destruction	
Name: Position: Signature: Date of Signature:	