Data Protection Impact Assessment for National Audit of Dementia HQIP NCA 2057 (NAD)

Document control:

	Name and role	Contact details
Document Completed by	**Chloë Hood**	**Chloe.hood@rcpsych.ac.uk**
Data Protection Officer name	**Richa Sharma**	**dataprotection@rcpsych.ac.uk**
Document approved by (this should not be the same person that completes the form).	**Richa Sharma/ Rebecca Danks**	**As above**
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	Z5702659	

Date Completed	Version	Summary of changes
12/02/20	**Draft 1**	**To indicate what will be completed when pilot data set is confirmed**
22/2/21	**Draft 2**	**Changes to the draft pilot data set and dates for spotlight audit**

Next review date: at pilot completion (currently planned for January 2022)

Contents

Screening questions

Please complete the following checklist:

	Section	Yes or No	N/A	Comments
1.	Does your project involve any automated decision making, evaluation or scoring including profiling and predicting using information about a person? Does the outcome from your project decide who gets access to services?	No		
2	Does your project involve any sensitive information or information of a highly personal nature?	Yes		Healthcare condition, assessments
3.	Does the proposal involve any data concerning vulnerable individuals who may be unable to easily consent or oppose the processing, or exercise their rights? 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		People living with dementia admitted to a general hospital
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		
5.	Does your project match data or combine datasets from different sources?	No		
6.	Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	Yes		Yes – pseudonymous service user data are collected from the participating Trusts/ Health Boards. Only member Trusts/ organisations are actively provided with our online privacy notice (though the privacy notice is publicly available online). NAD does not have direct contact with service users.

7.	Does your project process data that might endanger the individual's physical health or safety in the event of a security breach?	No		
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?	Yes		Changes to data set and sampling methodology

Data Protection Impact Assessment

This Data Protection Impact Assessment (DPIA) template and guide is a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. This tool will help organisations which process personal data to properly consider and address the privacy risk that this entails.

DPIA can be used alongside existing project management and risk management methodologies.

Conducting a DPIA is now a legal requirement under the GDPR (General Data Protection Regulation) which will start on the 25th of May 2018 and the new UK Data Protection Act. By completing a DPIA, this will help to ensure that your project is compliant with GDPR and UK data protection legislation. This document will be updated if further ICO guidance is published or there is change in legislation

A DPIA is the basis of a "privacy by design" approach, to help meet privacy and data protection expectations of customers, employees and other stakeholders. A DPIA is intended to be prospective and proactive and should act as an early warning system by considering privacy and compliance risks in the initial design and throughout the project.

Purpose and benefits of completing a DPIA

- A DPIA is a process which assists organisations in identifying and minimising the privacy risks of new projects or policies.
- Conducting a DPIA involves working with people within the organisation, with partner organisations and with the people affected to identify and reduce privacy risks.
- The DPIA will help determine the appropriate controls needed to protect personal data i.e. technical, procedural and physical.
- The DPIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Conducting a DPIA should benefit organisations by producing better policies and systems and improving the relationship between organisations and individuals.
- The ICO may often ask an organisation whether they have carried out a DPIA. It is often the most effective way to demonstrate to the ICO how personal data processing complies with Data Protection legislation.

Supplementary guidance

- Data Protection Impact Assessment under GDPR guidance
- ICO's conducting privacy impact assessments code of practice
- The ICO's Anonymisation: managing data protection risk code of practice may help organisations to identify privacy risks associated with the use of anonymised personal data.
- The ICO's Data sharing code of practice may help organisations to identify privacy risks associated with sharing personal data with other organisations.
- The ICO's codes of practice on privacy notices, as well as other more specific guidance, will also help an organisation to focus DPIAs on those issues.
- The Government Data Programme has developed a Data Science Ethical Framework to help organisations understand the benefits and risks of using personal data when developing policy. The Framework can be used as part of the process to help you describe information flows and identify privacy risks and solutions.

DPIA methodology and project information.

At what stage in the project did you conduct this DPIA? E.g. planning stage, changes to the existing project, in retrospect.

Planning stage

Describe the overall aim of the project and the data processing you carry out

2020 was planned as the pilot year for this round of the National Audit of Dementia, but the impact of the COVID-19 pandemic has resulted in long delays to the timeline. At this point only pilot sampling has been completed, and the data set has not been tested. This audit aims to provide comparable measurements of the quality of care for people with dementia admitted to general acute hospitals in England and Wales. Patient level information collected will be: Contextual pseudonymised information: Age Ethnicity First language Sex/gender Admitting condition Dates of admission and discharge Confirmed dementia or suspected cognition issues Subtype of dementia In addition we will collect information about items identified in consultation as priority for the quality of care

These will be focussed on key topic areas:

Measure	Data source
Median length of stay	Patient records/casenotes
Untoward incidents among people with dementia	DATIX records list of e.g. falls compared with audit sample, using Duplicate Values in Excel or similar

Quality of assessments for delirium screen, cognition and pain	Patient records
Presence of personal information document during admission	Bedside check
Initiation of discharge planning within 24 hours of admission	Patient records

In addition to this we will ask hospitals to trial collecting feedback directly from people with dementia. The method is to be confirmed, but is likely to be based on a flexible tool which can be used as a short questionnaire or as the basis for a semi-structured interview, carried out by dementia specialist clinicians, staff specialising in patient experience, or in some instances possibly by the family carer.

All eligible hospitals in England and Wales were due to be asked to carry out the carer survey in 2020, but this has been postponed with no date yet planned for resumption. This data collection uses the carer questionnaire developed and used in Rounds 3 and 4, returning over 4,500 responses in these rounds of audit. It involves distribution of paper questionnaires and online link to family and professional carers (e.g. from care home) visiting the person with dementia in hospital. The questionnaire has 10 questions, and produces 2 scores, for overall quality of care, and for quality of communication. It is anonymous, but collects personal information about the relationship to the person with dementia, age, ethnicity and sex/gender.

The project is also planning a spotlight audit to take place in community-based memory services. This will collect information about the services and from a sample of 50+ casenotes of patients whose initial assessment is from January 2021 – June 2021.

The casenote audit will collect contextual, pseudonymised information about the patient, and about key details of their assessment and diagnosis (types of assessment, waiting times, follow up)

Casenote audit questions have been previously developed for the NHS London led audit in memory services, but there will be additional questions looking at how assessment was carried out (e.g. virtually, face to face)

A questionnaire for patients/ family carers is planned, to look at the experience of assessment, especially the new ways of working/ different types of assessment offered.

The data set for this has been developed by Alzheimer's Society. It is anonymous and includes personal information about age, sex, ethnicity, memory service used (or borough of residence), relationship with the person with dementia and diagnosis.

DPIA Consultation

We advise you to consult with as many relevant people as possible (both internal and external stakeholders**)** while conducting this assessment, consultation is an important part of a DPIA and allows people to highlight privacy risks and solutions based on their own area of interest or expertise. Consultation can take place at any point in the DPIA process and may include the project management team, Data Protection Officer, designers, IT provider, procurement team, data processors, communications team, patients, stakeholders, corporate governance and compliance teams, researchers, analysts, statisticians, and senior management.

You must consult with the Data Protection Officer regarding the impacts on privacy. Please state below that you have.

If you decide against seeking the views of data subjects or their representatives e.g., this would be disproportionate or impracticable, then the justification must be made clear in the box below.

In the box below name the stakeholder group, date consulted and how consulted. Please insert another box if you consulted with many different stakeholder groups.

Standards consultation, circulated via professional and service user/ carer representative organisations, open to the public September-November 2019

Project Steering Group 18 December 2019, 27 January 2020, 18 January 2021

Project Implementation Group (input from clinical and patient/care adviser) every 1-2 months

Consultation with 6 Service User groups organised by Alzheimer's Society, December 2019- March 2020

Consultation with representations on Steering Group from people living with dementia/ carers: 3 meetings to date since July 2020.

Consultation with pilot sites: initial discussion about participation in January/ February 2020, followed by updated memorandum of understanding in August 2020, ad hoc meetings and pilot feedback workshop in December 2020.

Consultation with memory services (online webinars) about utility of data collection/ reflecting new ways of working – September-October 2020

Spotlight Audit Working Group 3 meetings November 2020 – March 2021

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.

This will be published June 2021

Data Information Flows

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.

	Communications Mailing List	**Registered Trust/Organisation Audit Contacts**	**Casenote audit (main audit and spotlight audit)**	**Patient/ carer questionnaire (spotlight audit)**	**Carer questionnaire (main audit)**	**Carer prize draw**
Data source	Individual request, service contact mapping exercise (online information)	Submission from Trust/organisation via registration form. Minor amendments via email occasionally.	Submission from Trust/organisation via online form.	Submission by patients and carers via online form.	Submission by carer (of person with dementia admitted to hospital) via paper copy with prepaid envelope provided, or via secure online link	Carer prize draw entry via postcard or online link
Output	Correspondence (emails, letters)	Correspondence (emails, letters)	Reports (National, Local and regional)	Reports (National and Local)	Reports (National, Local and regional)	List of winners (once draw has taken place
Data shared with	N/A	N/A	StatsConsultancy – external statistician will be sent anonymised sections of data for analysis	StatsConsultancy – external statistician will be sent anonymised sections of data for analysis	N/A	N/A. The information is not accessible by the NAD team until the draw takes place, but arrangements are made to ensure that it is not shared – see Comments
Contains identifiable personal information?	Yes	Yes	Yes – Pseudonymised (identification only possible by submitting Trust/organisation)	No	No	Yes
Contains sensitive information?	No	No	Yes (see details below in section Justification for collecting personal data)	Yes (see details below in section Justification for collecting personal data	Yes (see details below in section Justification for collecting personal data)	No
Electronic Storage	Yes On network drive (with restricted access)	Yes On network drive (with restricted access)	Yes On network drive (with restricted access)	Yes On network drive (with restricted access)	Yes On network drive (with restricted access)	No – information deleted once download made for draw

	On Dot Mailer account (accessible only with username and password) Shared email account (with restricted access)	On Dot Mailer account (accessible only with username and password) Shared email account (with restricted access) Formic collects submitted forms (accessible only with username and password)	Netsolving collects submitted forms (accessible only with username and password) Snap Surveys collects submitted forms as above (spotlight audit) Pseudonymous data may be downloaded by project team working remotely to RCPsych encrypted device or laptop. Downloaded data remains encrypted and within a secure environment.	Netsolving collects submitted forms (accessible only with username and password) Snap Surveys collects submitted forms as above (spotlight audit) Anonymous data may be downloaded to an encrypted device, remains encrypted and within a secure environment	Formic collects submitted forms (accessible only with username and password) Anonymous data may be downloaded to an encrypted device, remains encrypted and within a secure environment	
Paper/Hard copy storage	No	No	No	No	Yes Stored in team office cupboard which is locked when unattended, destroyed via confidential waste disposal	Yes – as above during submission period, and securely shredded once draw has taken place
Comments						Carers can win one of 5 £50 vouchers. Entries are separate to and cannot be linked with questionnaires – no common information on documents or in data collection systems. Postcards delivered to a dedicated box, and unseen by anyone, until winners are drawn. Online entries are submitted via a separate form which cannot link to questionnaire and

						unseen by anyone until the draw. The download of the information is carried out at the completion of the data collection. Entries are on a voluntary basis

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).

Formic software uses only UK data centres which comply with ISO 27001.

Snap Webhost survey data is held on servers n the UK. Snap surveys will only use hosting providers who are certified to ISO 27001:2013. Those hosting providers may also have Tier IV facilities, SSAE-16 and ISAE 3402 compliance, SOC II reports or PCI DSS compliance.

Net Solving – servers selected for project data will be within the UK and ISO compliant.

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	No		
NHS number	No		At this stage we do not plan to collect NHS numbers or other identifiable data. The process of piloting may demonstrate that this information is necessary in order to efficiently link separate data items pertaining to individual patients. In these circumstances, we will make Section 251 and other relevant applications for authorisation.

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]*
Address	No		
Postcode	No		
Date of birth	No		
Date of death	No		
Age	Yes		To assess the age range and demographics of the individual hospital cohorts. To assess whether elements of care quality such as the delivery of particular assessments varies with age.
Sex	Yes		To assess the breakdown by sex of the individual hospital cohorts. To assess whether elements of care quality such as the delivery of particular assessments varies with sex.
Marital Status	No		
Gender	Yes		To assess breakdown by gender (if different to sex) of the individual hospital cohorts. To assess whether elements of care quality such as the delivery of particular assessments varies with gender.
Living Habits	No		
Professional Training / Awards	No		
Income / Financial / Tax Situation	No		
Email Address	No		
Physical Description	No		
General Identifier e.g. Hospital No	No		
Home Phone Number	No		
Online Identifier e.g. IP Address/Event Logs	No		
Website Cookies	Yes		Formic software uses cookies indicate previous responses to some types of survey (for example use of usernames) and enhance the functionality of the tools. The cookies used on the Formic tools do not collect personal information. Snap surveys: as above Netsolving: as above
Mobile Phone / Device No	No		
Device Mobile Phone / Device IMEI No	No		
Location Data (Travel / GPS / GSM Data)	No		

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]*
Device MAC Address (Wireless Network Interface)	No		
Sensitive Personal Data			
Physical / Mental Health or Condition	Yes		Patients/ patient notes will be identified by the hospital using specific diagnoses/ criteria to ensure the patient level audit includes those who have confirmed or suspected diagnosis of dementia. Pilot sampling will also request information about admitting condition, dementia sub type and presence of delirium to ensure that the samples assembled using the new method are sufficiently comparable across sites. Main audit is also likely to collect this information so that case mix adjustment, if relevant, can be applied, and to further analyse whether admitting condition etc has an impact on the delivery or timing of assessments or other elements of care. The spotlight audit will also collection information on referral, assessment and diagnosis.
Sexual Life / Orientation	No		
Family / Lifestyle / Social Circumstance	No		
Offences Committed / Alleged to have Committed	No		
Criminal Proceedings / Outcomes / Sentence	No		
Education / Professional Training	No		
Employment / Career History	No		
Financial Affairs	No		
Religion or Other Beliefs	No		
Trade Union membership	No		
Racial / Ethnic Origin	Yes		To assess the age range and demographics of the individual hospital cohorts. To assess whether elements of care quality such as the delivery of particular assessments varies with ethnicity.
Biometric Data (Fingerprints / Facial Recognition)	No		
Genetic Data	No		
Spare			
Spare			

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]*
Spare			

Data quality standards for personal data

In the box below, describe how you will ensure that personal data is accurate and kept up to date.

National Audit of Dementia pilot will collect data from records of people with dementia identified during their admission to hospital and from hospital Datix records. The information, broadly described in Project information above, will be required at a given time point, to be determined by pilot. Carer questionnaires are collected over a specified 5-month time period and ask for the opinion of responders at the time of response. Individuals cannot be identified or contacted, and the information is not suitable for update.

Post submission, a data cleaning process will be carried out. This will highlight discrepancies between expected and received data. In addition, a random sample of Trusts/organisations will be selected to be visited by the audit team who will review the submitted data and case notes of a randomly selected cohort of service users.

We anticipate that a number of duplicate entries will be required as part of data submission to assess inter-rater reliability. The first five cases will be double audited from each Trust/organisation for this purpose.

Contact information will be kept update manually (by amendment, removal etc.) by the team, or the subscription process in bulk mailout software, Dot Mailer.

Access to the data highlighted above in the data information flow section, is restricted to those within the audit team. Data is saved on secure, access restricted drives, software and in email accounts, which cannot be accessed by those outside the team and organisation. Data shared with external contractors (e.g. external statistician) is anonymised and sent via secure encrypted email. Our contracts with our external data processors stipulate storage, confidentiality and access requirements.

Individual's rights

If your project uses personal data you must complete this section.

If your project uses personal data you must state how fairness and transparency will be achieved e.g. privacy notices on websites, posters, and leaflets. The information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Any information provided to children should be in such a clear and plain language that the child / vulnerable person can easily understand.

In the box below, please define the way you have ensured that individuals are aware of the rights, if they request those rights how will they achieve them? For example if an individual requests a copy of their information held by you, describe how you would do this. You can insert any relevant policy or process guides in the appendix at the end of this document if they are not already available on your website. This section does not refer to the personal information held about your audit staff.

Individuals rights (where relevant)	**Describe how you ensure individuals are aware of these rights**	**Describe how you would do this**	**Please copy and paste section of document that states the individual's rights**
Individuals are clear about how their personal data is being used.	e.g. Included in Privacy notice	e.g. Publish this to our website, please include web links.	Undergoing update
Individuals can access information held about them	Included in Privacy notice. Service user and questionnaires include description of how data is being used. Posters and postcards used to publicise the audit and use. Also includes information on how the audit will use individual comments and how the audit will be reported.	Privacy notice on website and will be sent to participating Trusts etc. Questionnaires given in hard copy or online with information. Audit packs include publicity materials.	https://www.rcpsych.ac.uk/about-us/data-protection/privacy-notice-national-audits **Sources of information used by national clinical audits** Information about a service users care is submitted to the relevant audit by the NHS Trusts or organisations providing NHS-funded care, providing care to the service user. The majority of the information is collected from hospital records, although some may be collected specifically for the purpose of the audit. Data is submitted via a secure web-based tool. Security and confidentiality is maintained through the use of passwords and registration process. Information submitted about service users' care is pseudonymised. The national clinical audit teams cannot identify the individual

			service user from the information they receive. The individual NHS Trusts or organisations providing NHS-funded care, hold the information needed to link a particular service **What will we do with the information you provide to us?** All of the information you provide will only be used for the purpose for which you provided it or to fulfil business, legal or regulatory requirements if necessary. The national clinical audits will not share any of the information provided to us with any third parties for marketing purposes. Information is held in secure data centres in the EU and US which comply with ISO 27001 security standards. The information you provide will be held securely by us and/or our data processors whether the information is in electronic or physical format. All of the data is accessible only to staff members working on the individual audit and data processors by approval. All audit data is held within restricted areas, is password protected and encrypted. The national clinical audits publish reports on the aggregated data at NHS Trust/organisation, Clinical Commissioning Group (CCG), regional and national levels at specific points during the audit programme. **What information do we ask for, and why?** The national clinical audits do not collect more information than we need to fulfil our stated purposes

			and will not retain it for longer than is necessary. The information we ask for is used to either maintain a record of you and to contact you, or for the purpose of assessing compliance against the agreed audit standards and providing benchmarked reports on compliance and performance. We process: demographic data including age, sex, ethnicity equal opportunities information. This is not mandatory information – if you don't provide it, it will not affect your status with the College. This information will not be made available to any staff outside of the College in a way which can identify you. Any information you do provide, will be used only to produce and monitor anonymous equal opportunities statistics and to promote diversity and equality. care data including date and time of admission, interventions received (e.g. medication, psychological therapies), processes of care outcome data including date of discharge, re-admission, discharge destination **Your rights** Under the Data Protection Act 2018, and General Data Protection Regulation (GDPR) you have rights as an individual which you can exercise in relation to the information we hold about you. **What if I do not want my information used by the audit?** Service users can choose to opt-out of the audit. Opting out of the audit will not affect the care a service user receives.

			For more information about how to opt-out of the audit, please contact your local NHS Trust/organisation directly as the audit teams do not hold service user identifiable information.
Request erasure (right to be forgotten) in certain circumstances, making clear that it does not apply to an individual's health or care record, or for public health or scientific research purposes	N/A – cannot identify individuals at national audit team level. Requests would be directed to Trusts.		
Rectification of inaccurate information	N/A – cannot identify individuals at national audit team level. Requests would be directed to Trusts.		
Restriction of some processing	N/A – cannot identify individuals at national audit team level. Requests would be directed to Trusts.		
Object to processing undertaken on some legal bases	N/A – cannot identify individuals at national audit team level. Requests would be directed to Trusts		
Complain to the Information Commissioner's Office;	Would facilitate this as much as possible (e.g. by publicising contact details) but we cannot identify individuals at national audit team level. Requests would be directed to Trusts.		
Withdraw consent at any time (if processing is based on consent)	N/A		
Data portability (if relevant)	N/A		
Individual knows the identity and contact details of the data controller and the data controller's data protection officer	Included in privacy notice.		

In which countries the data controller is processing their personal data. For data transfers outside the EU, a description of how the data will protected (e.g. the recipient is in an 'adequate' country / how a copy of the safeguards can be obtained.	Included in privacy notice		
To know the legal basis under their information is processed. Is there a clear legal basis for the processing of personal data? If so, what is the legal basis?	Privacy notice		
To know the purpose(s) for the processing of their information.	Included in privacy notice		
Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the personal data.	Included in privacy notice		
The source of the data (where the data were not collected from the data subject)	Included in privacy notice		
Categories of data being processed	Included in privacy notice		
Recipients or categories of recipients	Included in privacy notice		
The source of the personal data	Included in privacy notice		
To know the period for which their data will be stored (or the criteria used to determine that period)	Included in privacy notice		
The existence of, and an explanation of the logic involved in, any automated processing that has a	N/A		

significant effect on data subjects (if applicable)			

Privacy Risks

Types of Privacy risks

- Risks affecting individuals or other third parties, for example; misuse or overuse of their personal data, loss of anonymity, intrusion into private life through monitoring activities, lack of transparency.
- Compliance risks e.g. breach of the GDPR
- Corporate risks (to the organisation), for example, failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of patients or the public.

Risks affecting individuals

Patients have an expectation that their privacy and confidentiality will be respected at all times, during their care and beyond. It is essential that the impact of the collection, use and disclosure of any patient information is considered in regard to the individual's privacy.

In the box below insert the number of individuals likely to be affected by the project. This could be the number of unique patient records your project holds now and how many more records you anticipate receiving each year.

We are piloting a new sampling method and at this date it is not clear how many records will be identified. The previous round of audit identified 9782 individual records and in addition received 4736 questionnaires from carers. Spotlight audit in memory services is likely to identify up to 6,000 records. The patient/ carer questionnaire has not been developed/ tested. We will aim for10+ per service at least.

Please complete the table below with all the potential risks to the Individuals of the information you hold on them, your corporate risks and compliance risks.

When completing the table you need to consider if:

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Corporate and compliance risks

In the table, list the corporate risks to your organisation which could include reputational damage, loss of public trust, financial costs and data breaches. Below these, insert any compliance risks.

Possible corporate risks include:

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Examples of compliance risks include:

- Non-compliance with the common law duty of confidentiality
- Non-compliance with the GDPR.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.

Managing Privacy and Related risks

There are many different steps you can take to reduce a privacy risk. For example

- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors that will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Use your project plan and a detailed explanation of information flows to identify more precisely how a general risk may occur. For example, there may be particular points in a process where accidental disclosure is more likely to happen.

The DPIA actions should be added to into your project plan and risks added to your contract review documentation.

Privacy Risks and Actions Table

Please see appendix 2 for additional guidance on completing this table

What are the potential risks to the individuals whose personal data you hold?	**Likelihood of this happening** 1 Very unlikely 2 Unlikely 3 Possible 4 Likely 5 Very Likely (See guidance below for definition))	**Impact** 1 -Insignificant 2-Minor 3-Moderate 4-Major 5-Catastrophic (See guidance below for definition)	**Overall risk score** (likelihood x impact = score)	**Will risk be accepted, reduced or eliminated?**	**Mitigating action to reduce or eliminate each risk OR Where risk is accepted give justification.**	**Explain how this action eliminates or reduces the risk**	**Expected completion date**	**Responsible owner**
You should include illegitimate access, undesired modification and disappearance of data								
Access by a non-authorised external agency/individual	2	2	4	**A**	Data is pseudonymised and cannot be linked to an individual or Trust/organisation without additional information.	In the event of unauthorised access no individual could be identified	Complete d	CH
Access by a non-authorised internal College staff member	3	2	6	**R**	Review those who have access to folders and ensure only those who require access have it. Add passwords to files which are highly sensitive	Reduced number of people who may access information.	Ongoing for review as data collected	CH
External data hosting (Snap, Dot Mailer) have data breach	2	2	4	**A**	Contracting with external data hosting ensures that external system providers have high levels of security in place		Complete d	CH

					and are compliant with international data security standards			
Data sent to incorrect person	2	2	4	R	All emails to be checked in shared account by staff member. Macro ensures hospital code is matched to recipient Passwords to be added to sensitive files	Double checking reduces likelihood of error. Use of Macro eliminates possible human error in returning local reports Password protecting sensitive documents restricts access should it be sent	Complete d	CH
Corporate risks & compliance risks section								
Overall governance/ legal	1	Unknown	1		We are not aware of any governance or legal risks attendant on this project. Risk management for the College as a whole is governed by the Board of Trustees which has responsibility for ensuring the College maintains comprehensive risk			

					management systems and that appropriate actions are being taken to manage and mitigate risks. The Finance Management Committee (FMC) monitors and reviews these risk management arrangements every quarter and reports to the trustees on their effectiveness. College risk management policy aligns to Charity Commission guidelines (CC26). The Board of Trustees also reviews the established system of internal controls that fall within the Risk Management Policy. These controls have been designed to provide a reasonable level of assurance against the risk of error, fraud, and inappropriate or			

					ineffective use of resources. The College publishes an annual report with a statement of activity and Treasurers report in accordance with FRS 102.			
Data storage and confidentiality risks	1	4	4	R	Risks to confidentiality are greatly reduced by pseudonymisation of all data received so that no individual is identifiable in the data we hold. Data security policies and measures are aligned with bank-level and NHS provisions. Data will not be held in areas or on devices that are not protected. No unprocessed data will be handled externally. Any external analysis will be carried out with fully anonymised data sets and under guarantee of confidentiality.			

Regularly reviewing the DPIA

DPIA should be an ongoing process and regularly reviewed during the lifecycle of the project or programme to ensure

- Risks identified are still relevant
- Actions recommended to mitigate the risks have been implemented and mitigating actions are successful

You must add to your DPIA every time you make changes to the existing projects, send an updated version to your HQIP project manager and ensure that you incorporate any identified risks/issues to your risk/issue registers of the project contract review form.

Appendix 1 Submitting your own version of DPIA

If submitting your own version of DPIA please ensure it includes the following items. If any items are missing please add this to your DPIA and then submit it. You must also complete the screening questions above.

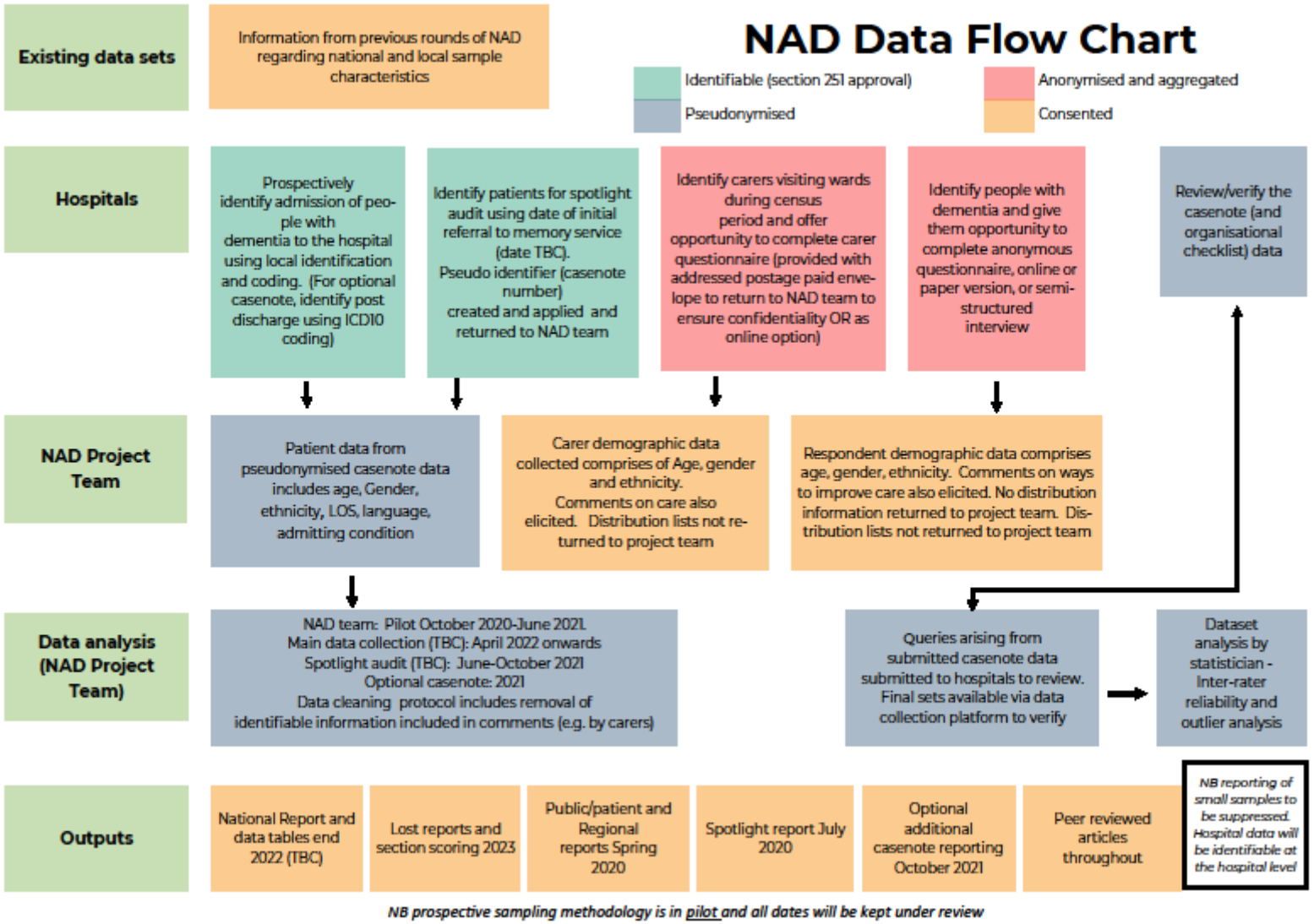
	Checkbox – Please tick	Evidence – Page number and section in your DPIA
Confirmation of advice /consultation sought from Data Protection Officer whilst completing the DPIA		
Name of DPO		
Name and role of person approving completion of DPIA form. This must not be the same person that completes the form.		
Will the DPIA be published or part of it such as the summary or conclusion (not essential but encouraged). If so, where is it published?		
Does it include a systematic description of the proposed processing operation and its purpose?		
Does it include the nature, scope, context and purposes of the processing		
Does it include personal data, recipients and period for which the personal data will be stored are recorded		
Does it include the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels)		
Does the DPIA explain how each individual's rights are Managed? See section on individuals rights		
Are safeguards in place surrounding international transfer? See section on sending information outside the EEA		

Was consultation of the document carried out and with whom?		
Organisations ICO registration number		
Organisations ICO registration expiry date		
Version number of the DPIA you are submitting		
Date completed		

Appendix 2 Guidance for completing the table

<table>
<tr><td>What are the potential risks to the individuals whose personal data you hold?</td><td>See examples above</td></tr>
<tr><td>Likelihood of this happening (H,M,L)</td><td>
<table>
<tr><th>Likelihood score</th><th>Description</th><th>Example</th></tr>
<tr><td>1</td><td>Very unlikely</td><td>May only occur in exceptional circumstances</td></tr>
<tr><td>2</td><td>Unlikely</td><td>Could occur at some time but unlikely</td></tr>
<tr><td>3</td><td>Possible</td><td>May occur at some time</td></tr>
<tr><td>4</td><td>Likely</td><td>Will probably occur / re-occur at some point</td></tr>
<tr><td>5</td><td>Very likely</td><td>Almost certain to occur / re-occur</td></tr>
</table>
</td></tr>
<tr><td>Impact (H,M,L)</td><td>
<table>
<tr><th>Impact scores</th><th>Description</th><th>Example</th></tr>
<tr><td>1</td><td>Insignificant</td><td>No financial loss; disruption to day to day work manageable within existing systems, no personal data loss/ no breach of confidentiality</td></tr>
<tr><td>2</td><td>Minor</td><td>Minor (<£100k) financial loss / disruption to systems; procedures require review but manageable; limited slippage in work activity, breach of confidentiality where < 20 records affected or risk assessed as low where data pseudonymised/files encrypted and no sensitive data</td></tr>
<tr><td>3</td><td>Moderate</td><td>Disruption to financial systems (<£250k); significant slippage in work activity or resources e.g. delay in recruiting staff; procedures and protocols require significant review, breach of confidentiality/ loss personal data where < 100 records involved and no sensitive data</td></tr>
<tr><td>4</td><td>Major</td><td>Major financial loss (£500k); large scale disruption to deliverables & project plans; business activity severely undermined, wasting considerable time / resources; poor quality report leading to loss of confidence in provider / HQIP / NHSE, breach of confidentiality/loss of personal sensitive data or up to 1000 records</td></tr>
</table>
</td></tr>
</table>

	5	Catastrophic	Huge financial loss (>£500k); significant threat to viability of the organisation in total or in part; huge disruption to business activity; almost total lack of confidence in project provider / HQIP / NHSE, serious breach of confidentiality/loss of personal sensitive data >1000 records involved
Risk score (calculated field)	Please multiply the likelihood by the severity (likelihood x severity = risk score). This score will help to rank the risk so the most severe risks are addressed first		
Will risk be accepted, reduced or eliminated? (where risk is accepted give justification)	A = Accepted (must give rationale/justification) R = Reduced E = Eliminated		
Mitigating action to reduce or eliminate each risk	Insert here any proposed solutions – see managing privacy and related risks section above OR If a risk has been accepted please give justification here (The purpose of the DPIA is to reduce the risk impact to an acceptable level while still allowing a useful project to be implemented.)		
Explain how this action eliminates or reduces the risk	Describe how your proposed action eliminates or reduces the possible risk. You may want to assess the costs/resource requirements (i.e. purchasing additional software to give greater control over data access and retention) and balance these against the benefits, for example the increased assurance against a data breach, and the reduced risk of regulatory action and reputational damage.		
Expected completion date	What is the expected completion date for your proposed action? Ensure that DPIA actions are integrated into the project plan. You should continue to use the PIA throughout the project lifecycle when appropriate. The DPIA should be referred to if the project is reviewed or expanded in the future.		
Action Owner	Who is responsible for this action?		


NAD Data Flow Chart
Identifiable (section 251 approval)
Pseudonymised
Anonymised and aggregated
Consented
Existing data sets
Information from previous rounds of NAD regarding national and local sample characteristics
Hospitals
Prospectively identify admission of people with dementia to the hospital using local identification and coding. (For optional casenote, identify post discharge using ICD10 coding)
Identify patients for spotlight audit using date of initial referral to memory service (date TBC). Pseudo identifier (casenote number) created and applied and returned to NAD team
Identify carers visiting wards during census period and offer opportunity to complete carer questionnaire (provided with addressed postage paid envelope to return to NAD team to ensure confidentiality OR as online option)
Identify people with dementia and give them opportunity to complete anonymous questionnaire, online or paper version, or semi-structured interview
Review/verify the casenote (and organisational checklist) data
NAD Project Team
Patient data from pseudonymised casenote data includes age, Gender, ethnicity, LOS, language, admitting condition
Carer demographic data collected comprises of Age, gender and ethnicity. Comments on care also elicited. Distribution lists not returned to project team
Respondent demographic data comprises age, gender, ethnicity. Comments on ways to improve care also elicited. No distribution information returned to project team. Distribution lists not returned to project team
Data analysis (NAD Project Team)
NAD team: Pilot October 2020-June 2021
Main data collection (TBC): April 2022 onwards
Spotlight audit (TBC): June-October 2021
Optional casenote: 2021
Data cleaning protocol includes removal of identifiable information included in comments (e.g. by carers)
Queries arising from submitted casenote data submitted to hospitals to review. Final sets available via data collection platform to verify
Dataset analysis by statistician - Inter-rater reliability and outlier analysis
Outputs
National Report and data tables end 2022 (TBC)
Lost reports and section scoring 2023
Public/patient and Regional reports Spring 2020
Spotlight report July 2020
Optional additional casenote reporting October 2021
Peer reviewed articles throughout
NB reporting of small samples to be suppressed. Hospital data will be identifiable at the hospital level
NB prospective sampling methodology is in pilot and all dates will be kept under review