Data Protection Impact Assessment

for

National Audit of Dementia in Memory Assessment Services 2026

Contents

Data Protection Impact Assessment

Overview

If you're conducting a project that will use personally-identifiable information, whether you're collecting it or it's being given to you, or you want to use an existing store of data in a different way, you are required to complete a *Data Protection Impact Assessment* (DPIA). Examples of the sort of personal data which will attract a DPIA are: pseudonymised, special category (sensitive), healthcare, social care, financial, but this list is not exhaustive.

This document comprises two sections:

1. A set of screening questions to clarify whether a DPIA is required.
2. A template form for a DPIA, based on guidance issued by the Information Commissioner's Office (ICO).

Please refer to the annexes for help with completing the DPIA.

Section 1: Screening questions

These questions are intended to help you decide whether a DPIA is necessary. If you answer 'yes' to any of these, a DPIA is required. You should also consider completing a DPIA for projects which are already running where these screening questions may apply. You may expand on your answers as the project develops if you need to.

1. Does the project involve the collection of new information about individuals? *Re-use of data collected for a different purpose is covered by question 4.*	Yes – data will be extracted from the Mental Health Service Dataset (MHSDS), and Data Health and Care Wales Performance data, and Memory Assessment Services data collated by Health and Care Jersey
2. Does the project compel individuals to provide information about themselves or ask others to disclose it on their behalf? *For example, a Trust providing data about an individual patient's care.*	Yes – data is submitted by Trusts/ Health Boards and to the MHSDS and DHCW. NAD is requesting access to these routine datasets. Health and Care Jersey is collating data into a routine dataset for the purposes of audit and NAD will also request this data
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	No patient-level data will be made available to organisations or people who have not had routine access to it before. Data at the patient-level will only be viewable to the services for which that data is submitted. The only exception to this is the access obtained by NAD and its sub-processers, providers of the data collection platform and of statistical consultancy.
4. **Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?**	Yes – data from these sources are not currently used for national audit. Data will be analysed to provide local, regional and national level benchmarking against audit metrics.
5. **Does the project involve you using new technology that might be perceived as being privacy intrusive?** *For example, the use of biometrics, facial recognition or fingerprint technologies.*	No
6. Will the project result in you making decisions or taking action against individuals in ways that could have a significant impact on them?	No
7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations?	Yes – Data collected will include sensitive data relevant to an individual's care under mental health services including age, sex,

For example, health records, criminal records or other information that people would consider to be private. Or any sensitive personal data (see Annex 4).	gender, ethnicity, dementia diagnosis status, treatment and interventions. NAD will also collect Lower Super Output Area Data to carry out analysis of relative deprivation in relation to service performance.
8. Will the project require you to contact individuals in ways that they may find intrusive?	No, the project will have no direct contact with any users of the services.
9. Does the project 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, or patients.*	Yes – NAD collects data relating to people who have memory problems and are assessed and diagnosed with dementia. This will include people who are elderly and/ or have a disability and may include people who lack capacity to consent to care.
10. Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	Yes – The data will be obtained by requesting access to routine datasets as above, containing information submitted as part of clinical care.

Section 2: Data Protection Impact Assessment Form

Step one: Identify the need for a DPIA

Explain what the project aims to achieve and what the benefits will be to the College, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a DPIA was identified drawing on your answers to the screening questions.

The National Audit of Dementia (NAD) is commissioned by the Healthcare Quality Improvement Partnership (HQIP) on behalf of NHS England and the Welsh Government and is part of the National Clinical Audit and Patient Outcomes Programme (NCAPOP). It is managed by the Royal College of Psychiatrists College Centre for Quality Improvement (CCQI) working in close partnership with professional and service user representatives.
In 2025-27, NAD is commissioned to carry out audit within Dementia diagnostic services including community based memory assessment services.

NAD aims to assess whether patients living with dementia and receiving care and treatment in audited services receive consistent, high-quality care, defined in terms of professionally agreed guidelines and standards. The audit covers England, Wales and Jersey.

Data prospectively identified for collection, analysis and reporting as key metrics, reflect existing national priorities drawn from guidance and confirmed following consultation with the Steering Group, local audit leads and people with lived experience.

The Healthcare Quality Improvement Plan (HQI plan) sets out 8 key metrics, including **5 healthcare improvement goals**. These are draft metrics which have received initial sign off by NHS England and Welsh Government. They are subject to amendment following testing of the data for quality and completeness.

Goals:

1) Reduce the average waiting time between referral to a diagnostic service and the patient receiving a diagnosis.
2) Increase the proportion of services with access to Picture Archiving and Communication System (PACS) to view structural imaging to diagnose dementia.
3) Decrease the variation between services in reporting diagnosis by dementia type
4) Increase the proportion of patients receiving Cognitive Stimulation Therapy (CST)
5) Increase the proportion of patients receiving post diagnostic monitoring

Draft key metrics are derived from:

- patient-level data from the health records of people living with dementia diagnosed by community based memory assessment services, managed by Mental Health Trusts in England, Health Boards in Wales and Health and Care Jersey
- Service level data pertaining to facilities in community based memory assessment services, as above

The processing affects users of these services: People living with memory problems or dementia, their cares and families; Healthcare professionals working within these services; Mental Health Trusts and Health Boards; Commissioners of services; commissioners of the audit

Data derived from the information collected for the clinical care record is essential to measure and report progress against these priority goals – e.g. dates of referral and diagnosis.

Data processed for this audit will be routinely collected data of individuals who have accessed memory assessment services, already collected and collated in the dataset MHSDS (England) or DHCW (Wales). These are individuals who will have or are undergoing assessment for a diagnosis of dementia, meaning that they are defined as vulnerable under the DPIA.
Data will be collected related to the metrics:

- Dates of referral, assessment, diagnosis
- Record of physical assessments: books, falls history, hearing, eyesight, smoking status, alcohol consumption
- Diagnosis and details of diagnosis (e.g. Mild Cognitive Impairment; dementia and type of dementia e.g. Alzheimer's Disease)
- Record of Cognitive Stimulation Therapy
- Record of named carer advisor
- Record of dementia care plan

Demographic data will be collected in order to assess whether elements of care quality such as the length of waiting times, delivery of particular assessments or care plan, varies with factors including ethnicity.
Demographic date will include:

- Age
- Sex
- Gender
- Ethnicity
- Lower Super Output Area

The data will be obtained by data access request submitted by the audit project on behalf of the Royal College of Psychiatrists to NHS England and to Welsh Government, and to Health and Care Jersey, in line with their requirements

Reporting against the refined metrics will take place for the first time end 2026 following data collection commencing in April 2026. Following evaluation, the audit may then move to repeat data collection at higher frequency enabling 6 monthly or quarterly reports for services to measure their progress. Data will be published on an interactive online dashboard. The dashboard will provide services with an overview of their performance at national, regional, and local levels. Services will be able to compare their performance across teams and services within their Trust/region, accessing run charts to identify trends in their data. Aggregated data will be made available to the public.

In 2026, a 'state of the nation' report will be produced, summarising national trends in the data and sitting alongside recommendations from the clinical and lived experience advisors

Data will be collected initially on a one-off basis, with evaluation to take place on moving to a quarterly frequency.

Rights of individuals with relation to data processed by National Audits is set out in our privacy notice Privacy notice national audits displayed on the website. This includes the legal basis for processing and the purpose of improving healthcare for individuals within the settings audited.

For these reasons a Data Protection Impact Assessment is essential.

The lawful basis for processing is

Data Protection Act DPA 2018 Schedule 1(1)(3) 'public health' underpinned by Health and Social Care Act 2012 Part 1 Section 2, which allows for data processing for health or social care purposes.

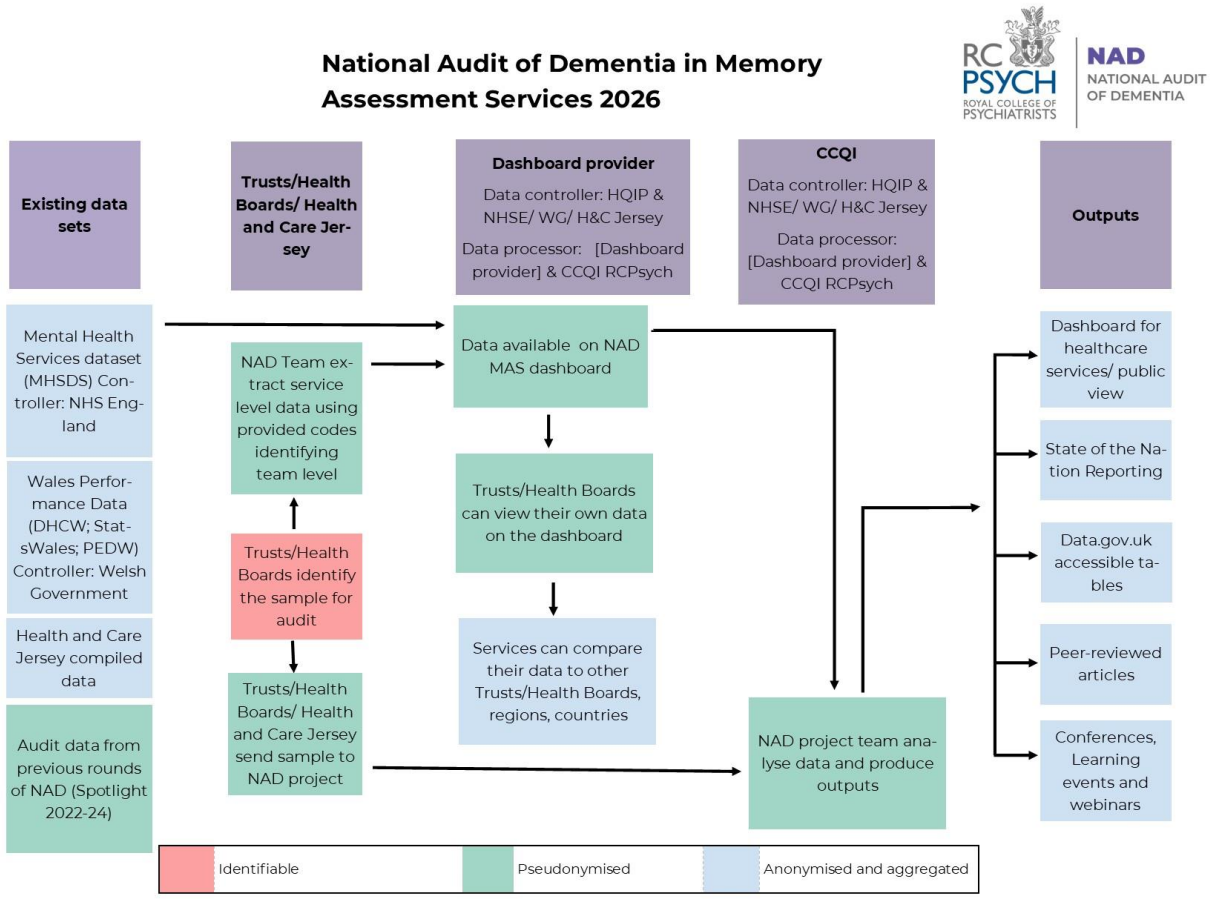
Article 6(1)(e) of the General Data Protection Regulation (GDPR) which allows for the processing of data where this is carried out in the public interest or in the exercise of official authority vested in our joint data controllers, HQIP and NHS England.

Article 9(2)(i) of the General Data Protection Regulation (GDPR) which allows for the processing of personal data for reasons of public interest in the area of public health, such as ensuring high standards of quality and safety of health care.

Step two: Describe the information flows

Please describe the collection, use and deletion of personal data here.

Include: where you are getting the data from, where it will be stored, where it could be transferred to, and the number of individuals likely to be affected. Please ensure you identify the Data Controller and Data Processor/s within the flows and any sub-contracted parties.



National Audit of Dementia Memory Assessment Services – patient level audit	
Data source	*MHSDS, DHCW and Health and Care Jersey data*
Output	- Online dashboard (local, regional and national level) - State of the nation report (December 2026) - QI learning workshops and webinars - Peer-review articles - Conference presentations
Data shared with	StatsConsultancy – external statistician will be sent pseudonymised sections of data for analysis. Dashboard provider TBC – online dashboard provider will be sent pseudonymised data for upload onto the platform. Lived Experience Advisory Group – aggregated/anonymised data will be shared with our Lived Experience Advisory Group, facilitated by Innovations in Dementia, to provide feedback on audit findings and co-produce outputs. Data will be aggregated and anonymised as per the public view available via the dashboard.
Contains identifiable personal information?	Yes – Identifiable and pseudonymised data Identifiable field(s): CareProfLocalTeamID – this field (in MHSDS) is **potentially** identifiable, as it is free text. No individually identifiable information such as name, address, NHS or other identification number will be **requested** by the audit.

Contains sensitive information?	Yes – Information relating to individuals' care under mental health services will be processed
Electronic Storage	Microsoft Azure Secure Server – Accessed only by named individuals within the CCQI granted security clearance. All information including any identifiable information will be transferred here for secure storage and pseudonymisation before export onto the RCPsych Sharepoint. RCPsych Sharepoint – Pseudonymised data will be transferred from the secure server onto the general server for processing and analysis. Dashboard provider TBC – Pseudonymised data will be uploaded onto the online data dashboard for the display of aggregated outputs.
Paper/Hard copy storage	No
Comments	

National Audit of Dementia Memory Assessment Services – patient/ carer feedback	
Data source	*Submitted online by people with dementia/ carers using memory assessment Services and providing experiential feedback*
Output	- Online dashboard (local, regional and national level) - State of the nation report (December 2026) - QI learning workshops and webinars - Peer-review articles - Conference presentations
Data shared with	StatsConsultancy – external statistician will be sent pseudonymised sections of data for analysis. Dashboard provider TBC – online dashboard provider will be sent pseudonymised data for upload onto the platform. Lived Experience Advisory Group – aggregated/anonymised data will be shared with our Lived Experience Advisory Group, facilitated by Innovations in Dementia, to provide feedback on audit findings and co-produce outputs. Data will be aggregated and anonymised as per the public view available via the dashboard.
Contains identifiable personal information?	No. This will not be requested and comments will be cleaned to ensure any potentially identifiable information is removed.
Contains sensitive information?	Yes. Ratings and comments of experience of using the service. Eg quality of care, communication, support.
Electronic Storage	Microsoft Azure Secure Server – Accessed only by named individuals within the CCQI granted security clearance. All information including any identifiable information will be transferred here for secure storage and pseudonymisation before export onto the RCPsych Sharepoint.

	RCPsych Sharepoint – Pseudonymised data will be transferred from the secure server onto the general server for processing and analysis. Dashboard provider TBC – Pseudonymised data will be uploaded onto the online data dashboard for the display of aggregated outputs.
Paper/Hard copy storage	No
Comments	

National Audit of Dementia Memory Assessment Services – service/ organisational audit	
Data source	Submitted online by participating services relating to service model and resourcing
Output	- Online dashboard (local, regional and national level) - State of the nation report (December 2026) - QI learning workshops and webinars - Peer-review articles - Conference presentations
Data shared with	StatsConsultancy – external statistician will be sent pseudonymised sections of data for analysis. Dashboard provider TBC – online dashboard provider will be sent pseudonymised data for upload onto the platform. Lived Experience Advisory Group –aggregated/anonymised data will be shared with our Lived Experience Advisory Group, facilitated by Innovations in Dementia, to provide feedback on audit findings and co-produce outputs. Data will be aggregated and anonymised as per the public view available via the dashboard.
Contains identifiable personal information?	No.
Contains sensitive information?	No
Electronic Storage	Microsoft Azure Secure Server – Accessed only by named individuals within the CCQI granted security clearance. All information including any identifiable information will be transferred here for secure storage and pseudonymisation before export onto the RCPsych Sharepoint. RCPsych Sharepoint – Pseudonymised data will be transferred from the secure server onto the general server for processing and analysis. Dashboard provider TBC – Pseudonymised data will be uploaded onto the online data dashboard for the display of aggregated outputs.

Paper/Hard copy storage	*No*
Comments	

Registered Trust/Organisation Audit Contacts	
Data source	Submission from Trust/organisation via registration form.
Output	Correspondence (emails, letters)
Data shared with	N/A
Contains identifiable personal information?	Yes
Contains sensitive information?	No
Electronic Storage	On RCPsych SharePoint (with restricted access)
Paper/Hard copy storage	No
Comments	

Step three: Consultation requirements

Explain what practical steps you will take to ensure you identify and address Data Protection risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the DPIA process. For example, 'Discussed storage with Information Security Team'.

Rationale for data collection (necessity and proportionality):
Key metrics, including those based on patient level data, were drafted by the NAD Clinical Leads Steering Group and based on national guidance and priorities (e.g. NICE Overview | Dementia: assessment, management and support for people living with dementia and their carers | Guidance | NICE; NCCMH nccmh-dementia-care-pathway-full-implementation-guidance.pdf), which themselves had included a process of consultation with service users, families, clinicians and other experts by experience. The NAD Steering Group includes clinical leads, patient and carer leads for the audit, National Clinical Director for Dementia, Healthcare professionals, charities and organisations representing people living with dementia or carers and healthcare professionals, representatives of NHS England, Welsh Government and HQIP.

Draft metrics were then discussed with the Lived Experience Reference Group, analytical leads at NHSE and clinical and analytic audit leads at individual Trusts, and volunteer panel of local audit leads; information leads at Health Boards; Senior Manager Quality, Safety and Performance Improvement, NHS Wales; Clinical Audit & Effectiveness Manager for Health & Care Jersey; before undergoing final amendment and confirmation by the Steering Group
Final draft metrics were then approved by NHSE and Welsh Government
Metrics are currently in draft version and subject to amendment depending on the outcome of data quality and feasibility testing.

Data storage and security:
GDPR requirements are a required topic of mandatory training for all staff members. Data requirements relating to phases of data collection and analysis are discussed within the team in relation to data cleaning, analysis, access and storage, with the college IS department and managers in relation to security and storage requirements, and generally with the Head of Research and Audit, the College Data Protection Officer, and other programme managers in relation to resourcing and compliance.

Step four: Identify the Data Protection and related risks

Identify the key Data Protection risks and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on a more formal risk register.

Use Annex 2 to help identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation/ corporate risk
Identifiable data are securely transferred from NHS England/ DHCW/ Health and Care Jersey onto the Microsoft Azure secure server	Personal identifiable data, could cause harm or distress if accessed/lost/shared	Data are subject to unlawful access or processing, if lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage
Identifiable data held on third party servers (Microsoft Azure)	Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost	Data are copied and/or retained longer than required, is subject to unlawful access or processing, or is lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.
Personal pseudonymous data uploaded to online dashboard to display analysis results	Personal and sensitive data, relating to an individual's health care and sensitive diagnosis, could cause harm or distress if accessed/shared/ lost	Data are subject to unlawful access or processing, if lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.
Sensitive, pseudonymous data held on third party servers (Dashboard provider TBC)	Personal, sensitive data, relating to an individual's health care and sensitive diagnosis, could cause harm or distress if accessed/shared/ lost	Data are copied and/or retained longer than required, is subject to unlawful access or processing, or is lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.
Sensitive pseudonymous data are stored on thousands of service users, which is copied across software files for analysis	Personal, sensitive data, relating to an individual's health care and sensitive diagnosis, could cause harm or distress if accessed/shared/ lost	Data are subject to unlawful access or processing, or is lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.
Identifiable or pseudonymous data (electronic) accessed by unauthorised staff at RCPsych	Personal, sensitive data, relating to an individual's health care and sensitive diagnosis, could cause harm or	Data are subject to unlawful access or processing, or is lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.

	distress if accessed/shared/ lost		
Pseudonymous datasets shared by email	Personal, sensitive data, relating to an individual's health care and sensitive diagnosis, could cause harm or distress if accessed/shared/ lost	Data are subject to unlawful access or processing, if lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.
Laptop containing personal data that is lost or stolen	Personal, sensitive data, relating to an individual's health care and sensitive diagnosis, could cause harm or distress if accessed/shared/ lost	Data are subject to unlawful access or processing, or is lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage
The wrong datasets are shared with members, containing data on service users from other organisations	Personal, sensitive data, relating to an individual's health care and sensitive diagnosis, could cause harm or distress if accessed/shared/ lost	Data are subject to unlawful access or processing, or is lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.

Step five: Identify solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary.

For example, the production of new guidance or future security testing for systems. Risks may include those affecting individuals, organisations or third parties (e.g. misuse or overuse of data, loss of anonymity etc.), compliance risks with GDPR or other relevant legislation, corporate risks (e.g. reputational, loss of trust of service users or the public).

- NAD team will request deletion of any data from Microsoft Azure to comply with Section 251 for handling identifiable information.
- Contract will be appropriately drawn up with dashboard provider (TBC) and is in place with Microsoft Azure, who hold appropriate security credentials: ISO 27001.
- Only RCPsych approved laptops are used with appropriate security protections.
- Pseudonymous datasets are stored on secure SharePoint with restricted access to project folders. Computer terminals time-out and require password access.
- No identifiable patient level data will be shared at any point post submission. Data will be pseudonymised or anonymised prior to analysis. Data will be aggregated for reporting and small numbers suppressed.
- Identifiable datasets are stored on Microsoft Azure servers (outside RCPsych system), and access will be granted only to named staff via remote desktop, allowing all access to be logged. Only pseudonymous versions of the dataset will be stored on RCPsych SharePoint.
- Policy is to review retention of datasets annually.
- Pseudonymous data held on third party servers (Dashboard provider TBC) deleted when no longer required.
- Identifiable data will be retained as per Section 251 approval, with any extension to this requiring revised Section 251 approval.
- All shared datasets are password protected; no identifiable data are returned to sites. Checking procedure in place within team for all datasets sent.

Step six: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Person Responsible and deadline for completion	Approved by
Identifiable data are securely transferred from NHS England/ DHCW/ Health and Care Jersey onto the Microsoft Azure secure server	Contract is in place with Microsoft Azure, who appropriate hold security credentials: ISO 27001.	Chloe Hood Programme Manager Ongoing	Philippa Nunn Head of Clinical Audits and Research
Identifiable data held on third party servers (Microsoft Azure)	Contract is in place with Microsoft Azure, who appropriate hold security credentials: ISO 27001.	Phil Burke, Head of IS Completed	Philippa Nunn Head of Clinical Audits and Research
	Only named RCPsych staff will have access to Microsoft Azure via remote desktop. All access will be logged	Phil Burke, Head of IS Completed	Philippa Nunn Head of Clinical Audits and Research
	Identifiable data will be retained as per Section 251 approval, with any extension to this requiring revised Section 251 approval.	Chloe Hood Programme Manager Ongoing	Philippa Nunn Head of Clinical Audits and Research
Datasets shared by email	All shared datasets are password protected.	Chloe Hood Programme Manager Ongoing	Philippa Nunn Head of Clinical Audits and Research
Sensitive, pseudonymous data held on third party servers (Dashboard provider TBC)	Data emailed are made anonymous. No identifiable information will be included in the datasets when emailed.	Chloe Hood Programme Manager Ongoing	Philippa Nunn Head of Clinical Audits and Research
Laptop containing pseudonymous data that is lost or stolen.	Only RCPsych approved laptops are used with appropriate security protections. No identifiable data are stored on laptops.	Chloe Hood Programme Manager Ongoing	Philippa Nunn Head of Clinical Audits and Research

Data (pseudonymous or identifiable) accessed by unauthorised staff at RCPsych	Pseudonymous datasets are stored on secure SharePoint with restricted access to project folders. Computer/laptop terminals time-out and require password access. Identifiable data are stored on Microsoft Azure servers. Only named RCPsych staff have access via remote desktop. All access is logged.	Phil Burke, Head of IS Completed	Philippa Nunn Head of Clinical Audits and Research
Sensitive data are collected on thousands of service users for the audit. Pseudonymous versions of the datasets are copied across software files retained for long-term statistical analysis	Pseudonymous datasets are stored on secure SharePoint with restricted access.	Phil Burke, Head of IS Completed	Philippa Nunn Head of Clinical Audits and Research
	Policy is to review retention of datasets annually.	Chloe Hood Programme Manager Ongoing	Philippa Nunn Head of Clinical Audits and Research
	Identifiable datasets are stored on Microsoft Azure servers. Only named RCPsych staff will have access to these. All access is logged. Identifiable data will be stored for the period granted by Section 251 approval.	Phil Burke, Head of IS Ongoing	Philippa Nunn Head of Clinical Audits and Research
	Contract will be drawn up with an approved supplier, who hold appropriate security credentials.	Chloe Hood Programme Manager Ongoing	Philippa Nunn Head of Clinical Audits and Research
Sensitive data held on third party servers - dashboard provider (TBC)	Only RCPsych staff have access to the raw data on the data dashboard (provider TBC). Teams will have access to their own pseudonymous data using a secure username, password and two-factor authentication process. All other data available to teams will be aggregated.	Chloe Hood Programme Manager Ongoing	Philippa Nunn Head of Clinical Audits and Research
	The NAD team will request data are deleted from servers of the	Chloe Hood Programme Manager	Philippa Nunn Head of Clinical

	dashboard provider (TBC) once no longer required.	Ongoing	Audits and Research

Step seven: Integrate the DPIA outcomes back into the project plan

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any Data Protection concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
NAD team will request dashboard provider (TBC) and Microsoft Azure to delete data retained, once no longer required.	Ongoing	Programme Manager
Contract is in place with dashboard provider (TBC)and Microsoft Azure who hold appropriate security credentials.	Completed	Programme Manager/ Head of IS
All shared datasets are password protected.	Ongoing	Programme Manager
Only RCPsych approved laptops are used with appropriate security protections	Completed	Head of IS
Data emailed are made anonymous. No identifiable information will be included in the datasets when emailed.	Ongoing	Programme Manager
Pseudonymous datasets are stored on secure SharePoint with restricted access to project folders. Computer terminals/ RCPsych laptops time-out and require password access.	Completed	Programme Manager
Policy is to review retention of datasets annually.	Ongoing	Programme Manager
After being held for 5 years, pseudonymous data will be made anonymous by deletion of unique patient identifiers.	Ongoing	Programme Manager
Identifiable data will be stored for the period allowed	Ongoing	Programme Manager

according to Section 251 approval. Any retention past this date will require further Section 251 approval.		

Annex 1

Primary contact for advice and guidance

Richa Sharma
Head of Membership Services and Faculties – Data Protection Officer
richa.sharma@rcpsych.ac.uk
020 3701 2589

Annex 2

The data protection principles and relevant questions

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the General Data Protection Regulation, Data Protection Act 2018 or other relevant legislation, for example the Human Rights Act.

Personal data shall be:

1. **processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');**

   a) Have you identified the purpose of the project?

   b) How will you tell individuals about the use of their personal data?

   c) Do you need to amend or create a new privacy notice/s?

   d) Have you established which conditions for processing apply?

   e) If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

   f) If your organisation is subject to the Human Rights Act, you also need to consider:

   g) Will your actions interfere with the right to privacy under Article 8?

   h) Have you identified the social need and aims of the project?

   i) Are your actions a proportionate response to the social need?

2. **collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');**

   a) Does your project plan cover all of the purposes for processing personal data?

   b) Have you identified potential new purposes as the scope of the project expands?

   c) Consider using the Data Categories table at Annex 4 to help you identify the purposes of your collection/processing – this may help you evaluate the scope of the data required for your project.

3. **adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');**

   a) Is the quality of the information good enough for the purposes it is used?

   b) Which personal data could you not use, without compromising the needs of the project?

4. **accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');**

   a) If you are procuring new software does it allow you to amend data when necessary?

   b) How are you ensuring that personal data obtained from individuals or other organisations is accurate?

5. **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');**

   a) What retention periods are suitable for the personal data you will be processing?

   b) Are you procuring software that will allow you to delete information in line with your retention periods?

6. **processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').**

   a) Do any new systems provide protection against the security risks you have identified?

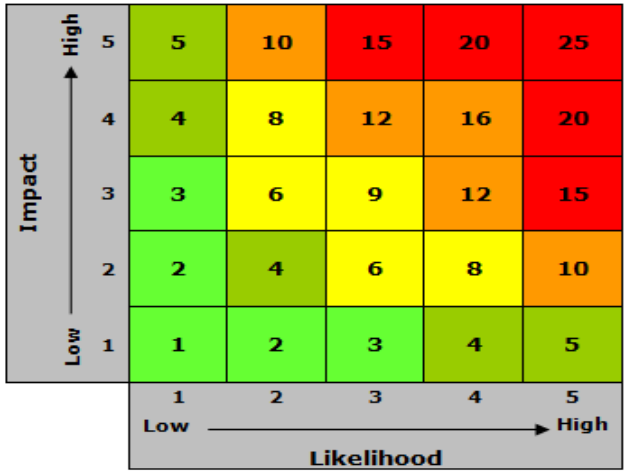
   b) What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Annex 3

Risk and Issues Log

Risk No	Risk Description	Likeli-hood	Severity of Impact	Raw Risk Score	Mitigation	Likelihood	Severity of impact	Residual Risk	Owner

1-3	Low likelihood & low severity of impact
4-5	Low / medium likelihood & low / medium severity of impact
6-9	Medium likelihood & medium severity of impact
10-16	Medium / high likelihood & medium / high severity of impact
15-25	High likelihood & high severity of impact



Annex 4

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		
Address	No		
Postcode	No		
Date of birth	No		
Date of death	No		
Age	Yes		To assess the age range and demographics of the individual service 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 service 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 service 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/Paris ID	No		
Home Phone Number	No		
Online Identifier e.g. IP Address/Event Logs	No		
Website Cookies	No		
Mobile Phone / Device No	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 Mobile Phone / Device IMEI No	No		
Location Data (Travel / GPS / GSM Data)	No		
Device MAC Address (Wireless Network Interface)	No		
Sensitive Personal Data			
Physical / Mental Health or Condition	Yes		Sampling will request information about referral to the service, assessment, diagnosis, dementia sub type. This will be essential to ensure comparable samples, compare sampling across services, and for case mix adjustment, where relevant.
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 service 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		
Use of Mental Health Legislation/DoLS etc.	No		
Care Data including interventions, procedures, surgery etc.	Yes		
Spare			

Document Information (Office use only)

Title of document	Data Protection Impact Assessment National Audit of Dementia in Memory Assessment Services 2026
Version number	1
Type of document	DPIA for CCQI Cluster 3 Audit Project
Purpose of document	To capture the impact of project related data collection including pseudonymised, special category (sensitive), healthcare, social care, financial (this list is not exhaustive).
Target audience	Audit commissioners: NHS England Welsh Government Healthcare Quality Improvement Partnership Audit Participants: Mental Health Trusts in England and Wales Health and Care Jersey Patients and public: Users of memory assessment services and families General public Governance: RCPsych Heads and Directors NAD Implementation Group NAD Steering Group Project Team
Distribution	NAD Website HQIP PODIO IG Update
Consultation	As above
Approved by	Philippa Nunn
Date of approval	29 January 2026
Author	Chloë Hood
Review date	Janaury 2027

Document Control (Office use only)

Version Number	Reason for Change	Description of Change	Date of Change	Author