Data Protection Impact Assessment

for

National Clinical Audit of Psychosis (NCAP)
2025-2027

Contents

Overview 3
Section 1: Screening questions 4
Section 2: Data Protection Impact Assessment 7
Step one: Identify the need for a DPIA 7
Step two: Describe the information flows 8
Step three: Consultation requirements 11
Step four: Identify the Data Protection and related risks 12
Step five: Identify solutions 14
Step six: Sign off and record the DPIA outcomes 15
Step seven: Integrate the DPIA outcomes back into the project plan 17
Annex 1 18
The data protection principles and relevant questions 18
Annex 2 21

Overview

This Data Protection Impact Assessment (DPIA) describes how the National Clinical Audit of Psychosis (NCAP) processes personal data for the purposes of delivering the audit. The DPIA sets out the types of data used, the lawful basis for processing, the data flows involved, and the measures in place to protect the rights and freedoms of individuals.

The document comprises two sections:

1. Screening questions to determine whether a full DPIA is required.
2. The DPIA template, based on guidance issued by the Information Commissioner's Office (ICO), which assesses the risks and safeguards associated with data processing for NCAP.

Supporting information is provided in the annexes, including data categories and data protection principles.

For operational queries about NCAP) please contact: ncap@rcpsych.ac.uk

For data protection queries relating to this DPIA or to the processing described within it, please contact the Royal College of Psychiatrists' Data Protection Officer at: DataProtection@rcpsych.ac.uk

Section 1: Screening questions

This section sets out the screening questions used to determine whether a Data Protection Impact Assessment (DPIA) is required for the National Clinical Audit of Psychosis (NCAP). These questions assess whether the project involves activities that present potential data protection risks and therefore require further assessment through a full DPIA.

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.*	No - for England, NCAP uses data already collected routinely within the Mental Health Services Dataset (MHSDS) and provided to us by NHS England. For Wales, there is currently no equivalent national dataset, so an interim national system has been established to extract the required data centrally and transfer it securely to NCAP. This means no new information is being collected directly from individuals.
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 – although NCAP does not compel individuals to provide any information directly, the audit does require NHS England and the Welsh Government to disclose pseudonymised patient-level data for audit purposes. These organisations are required to supply data extracted from national datasets as part of statutory and contractual arrangements. All data provided to NCAP is pseudonymised prior to transfer, and NCAP does not receive any information directly from individuals.
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Yes – pseudonymised information is disclosed to NCAP and its authorised processors, who would not otherwise have routine access to these datasets. This disclosure is made by NHS England and the Welsh Government, who are required to provide pseudonymised patient-level data for audit delivery. NCAP only receives pseudonymised data, and no direct identifiers are provided.

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 – while the information comes from data originally collected for the purpose of delivering and recording healthcare, NCAP uses this data for secondary purposes, including national, regional, organisational and team-level benchmarking and quality improvement analysis. This represents a different use from the original clinical purpose. The purpose is, however, aligned with public interest, healthcare quality improvement and national audit functions.
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 - NCAP does not make decisions about individuals or take actions affecting them; all outputs are aggregated and used only for service improvement, and no automated decision-making or profiling takes place.
7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? *For example, health records, criminal records or other information that people would consider to be private. Or any sensitive personal data (see Annex 4).*	Yes – the dataset contains sensitive health information, including mental health diagnoses, treatments and related outcomes. These are special category data and therefore carry higher privacy expectations. All data provided to NCAP is pseudonymised.
8. Will the project require you to contact individuals in ways that they may find intrusive?	No
9. Does the project involve any data concerning vulnerable	Yes – the dataset includes information about people accessing

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.*	mental health services, including children, older adults, and individuals who may lack capacity or otherwise be considered vulnerable. All data provided to NCAP is pseudonymised.
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 is sourced from national datasets (MHSDS/HES/ONS in England and an interim national system in Wales) rather than directly from individuals. NCAP does not have direct contact with individuals and therefore cannot provide privacy notices to them. NHS England applies national data opt-outs before supplying the data, and NCAP processes only pseudonymised information.

Section 2: Data Protection Impact Assessment

Step one: Identify the need for a DPIA

This step explains the purpose of the NCAP, the benefits of the project for organisations, individuals and wider stakeholders, and the reasons a Data Protection Impact Assessment is required. It summarises the aims of the project and outlines why a DPIA is necessary based on the responses to the screening questions.

The National Clinical Audit of Psychosis (NCAP) is commissioned by the Healthcare Quality Improvement Partnership (HQIP) as part of the National Clinical Audit and Patient Outcomes Programme (NCAPOP). Funded by NHS England and the Welsh Government, NCAP aims to improve the quality of psychosis care by assessing NHS Mental Health Trusts in England and Health Boards in Wales against evidence-based standards, supporting national and local quality improvement.

NCAP has been running since 2017 and transitioned fully to a routine dataset methodology in 2025, using national data sources such as the Mental Health Services Dataset (MHSDS) in England and an interim national data collection system in Wales. This approach reduces burden on services, supports more sustainable audit delivery and enables consistent, long-term benchmarking. The programme is now funded until July 2027 to continue this work.

The routine data audit uses pseudonymised MHSDS, HES and ONS data supplied by NHS England, with the eligible cohort identified using the CareProfTeamLocalID (M102905). This allows NCAP to monitor service performance, identify variation, and support improvements in the quality and equity of psychosis care. Participating services benefit from being able to benchmark their performance against national standards and comparable providers, while individuals and the public benefit indirectly from improved service quality.

Although Section 251 approval permits NCAP to receive identifiable data items such as NHS number, postcode and date of birth for linkage purposes, these identifiers are not currently provided to NCAP and are not used within the routine audit dataset, which remains fully pseudonymised.

A DPIA is required because the project involves processing large volumes of special category health data, including information relating to individuals who may be considered vulnerable. The data is drawn from national datasets rather than collected directly from individuals and is linked across multiple national sources for audit and quality improvement purposes. Pseudonymised datasets are also shared with contracted data processors and Clinical Advisors for audit delivery and analysis. These factors trigger

several of the DPIA screening criteria, confirming the need for a full assessment.

Step two: Describe the information flows

This step describes how personal data is collected, used, stored, shared and deleted within NCAP. It outlines the data sources, the organisations involved in controlling and processing the data, and the ways in which the information is transferred and managed throughout the audit process.

Data Controllers and Data Processors

- HQIP is the Data Controller for the audit programme.
- NHS England is the Data Controller for the source MHSDS/HES/ONS datasets (England)
- Improvement Cymru is the Data Controller for the interim Welsh dataset.
- The Royal College of Psychiatrists (NCAP) acts as the Data Processor for HQIP.
- Athera Healthcare is a sub-processor for dashboard hosting until April 2026; from April 2026 the dashboard is hosted internally within RCPsych's secure Power BI environment.
- Clinical Advisors may receive pseudonymised extracts as sub-processors.

Audit Dataset (Routine data)	
Data source	• England: Pseudonymised dataset derived from MHSDS, HES and ONS, provided to NCAP via secure transfer from NHS England. • Wales: Pseudonymised dataset extracted centrally using the interim national data collection system (in place until the national Welsh equivalent to MHSDS is developed). Data is securely transferred to NCAP at national level.
Output	• Secure online dashboard presenting aggregated national, regional, organisational and team-level data for England and Wales. • Authorised audit leads can also download pseudonymised patient-level data for their own team or service only, to support local quality improvement, validation and understanding of their results. These extracts do not contain direct identifiers

Data shared with	• Until April 2026: Pseudonymised datasets are shared with Athera Healthcare to host the NCAP dashboard. • From April 2026: The dashboard will be hosted internally within the RCPsych Power BI environment (no external processor). • Clinical Advisors: Receive pseudonymised, password-protected extracts as needed. • StatsConsultancy: Receives anonymised analysis extracts only.
Contains identifiable personal information?	No – NCAP does not receive direct identifiers (e.g., NHS number, name, date of birth). All data transferred to NCAP is pseudonymised. However, the dataset includes pseudonymous identifiers that may enable EIP teams to re-identify their own patients when NCAP provides team-specific extracts back to them for validation or quality improvement. NCAP itself cannot identify individuals from the data it holds. No – NCAP does not currently receive any direct identifiers (e.g., NHS number, date of birth). While Section 251 support is in place permitting NCAP to receive these identifiers for specific approved purposes (including dataset linkage), these identifiable items are not currently provided to NCAP. The routine audit dataset contains no direct identifiers. NCAP receives only pseudonymised records, which include Service Request IDs and other technical identifiers. These cannot be used by NCAP to directly identify individuals. Local teams may re-identify their own patients when NCAP provides team-specific extracts, but NCAP itself cannot identify any individuals from the data it processes.
Contains sensitive information?	Yes - includes special category health data relating to mental health diagnoses, treatments, interventions and outcomes. (see details below in Annex 4)
Electronic Storage	• Pseudonymised datasets are stored on the RCPsych SharePoint platform within restricted-access project folders. • Until April 2026, the NCAP dashboard is hosted on Athera Healthcare's secure platform. From April 2026 onwards, the

	dashboard will be hosted internally within the RCPsych secure Power BI environment (no external dashboard provider). • Egress is used for secure file transfer and encrypted storage where required. • Clinical Advisors may hold pseudonymised extracts on RCPsych-approved encrypted laptops, with password-protected files and strict access controls.
Paper/Hard copy storage	No
Comments	

Registered Trusts/Health Board audit contacts	
Data source	Contact details provided directly by individuals or gathered through service contact mapping exercises and publicly available organisational information (e.g., Trust/Health Board websites).
Output	Operational correspondence, primarily emails (and occasional letters), relating to audit participation, updates, guidance and reporting.
Data shared with	Not shared with any external organisations.
Contains identifiable personal information?	Yes – includes names, job titles, organisational details and email addresses of audit leads or service contacts.
Contains sensitive information?	No – no special category or patient data is included.
Electronic Storage	Stored on RCPsych SharePoint within restricted-access project folders, protected by corporate security measures and role-based access control.
Paper/Hard copy storage	No hard copies are created or stored.
Comments	The mailing list is used solely for managing communication with participating Trusts and Health Boards and does not include any patient-level information. It also serves as the source of audit leads and team contacts for participation and dashboard access, as NCAP no longer uses a separate registration process.

Step three: Consultation requirements

This step outlines the consultation undertaken to identify and address data protection risks associated with NCAP. It summarises the internal and external stakeholders involved in reviewing the data flows, governance arrangements and technical safeguards, and describes how consultation has informed the development and review of this DPIA.

- The NCAP team has reviewed College Information Governance (IG) policies and data-management processes with the internal project team.
- Guidance on GDPR and Data Protection Act 2018 requirements has been discussed with the RCPsych Data Protection Officer and GDPR leads.
- Secure storage, access controls and technical measures have been reviewed with the RCPsych IT and Information Security teams.
- NCAP will consult HQIP's Project Manager and HQIP's DPO/IG Lead during the DPIA review process and when proposing any material changes to data flows, processing arrangements or dataset content, in line with NCAPOP contract requirements.
- Consultation will take place through project governance meetings, written reviews, and email correspondence, and will form part of NCAP's annual DPIA review cycle.

Step four: Identify the Data Protection and related risks

This step outlines the key data protection, compliance and corporate risks associated with NCAP. It summarises the potential risks to individuals and the organisation arising from the processing of personal data and draws on the data protection principles set out in Annex 1.

	Privacy issue	Risk to individuals	Compliance risk	Associated organisation/ corporate risk
1.	**Processing large volumes of mental health data:** Large volumes of pseudonymised special category mental health data are processed and stored for audit purposes, including dashboard hosting and analytical use.	Personal data relating to mental health care could cause harm or distress if accessed, shared, or lost.	Unlawful access, processing, or data breach involving special category data.	Regulatory action, reputational damage, and loss of trust.
2	**Storage and processing on third party systems:** Pseudonymised datasets are held on Athera Healthcare's systems until April 2026, then migrated to RCPsych's Power BI environment.	Risk of unauthorised access or retention beyond required periods.	Failure to ensure processors follow GDPR requirements or failure to delete data when no longer needed.	Reputational damage and contractual non-compliance.
3	**Creation of multiple analytical**	Increased risk of accidental disclosure or loss.	Data may be subject to unlawful access,	Reputational impact in the event of mishandling.

	Privacy issue	Risk to individuals	Compliance risk	Associated organisation/ corporate risk
	copies of datasets: Analytical work may involve several working copies of pseudonymised datasets.		processing or disclosure in a breach, or retained longer than necessary if deletion processes are not followed.	
4	**Downloading data:** Authorised users (e.g., audit leads) downloading pseudonymised patient-level data for their own team.	Local re-identification possible at Trust/Health Board level; risk if local safeguards are insufficient.	Risk of inappropriate onward sharing or insecure local storage.	Could lead to regulatory fines, reputational damage.
5	**Loss or theft of RCPsych devices** holding pseudonymised extracts (e.g., Clinical Advisor laptops).	Potential exposure of sensitive data.	Failure to maintain device security.	Possible breach reporting, reputational damage.
6	**Incorrect dataset shared with a service** The wrong datasets are shared with members, containing data on service users from other organisations	Personal, sensitive data, relating to an individual's mental health, 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.
7	**Future identifiable data** if identifiable NHS numbers or other identifiers permitted under Section 251 are used in	Use of identifiable data creates potential for harm if breached; opt-out handling must be correct.	Misapplication of Section 251 approvals or national data opt-outs.	Could lead to regulatory fines, reputational damage.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation/ corporate risk
future, additional controls will be implemented.			

Step five: Identify solutions

This step describes the measures in place to mitigate data protection risks associated with NCAP, as well as any planned actions to strengthen safeguards. It outlines the technical, organisational and procedural controls used to protect personal data and ensure compliance with data protection legislation.

Pseudonymised datasets are stored on restricted-access RCPsych SharePoint sites and, from April 2026, within RCPsych's secure Power BI environment (following migration from Athera Healthcare).

- Access to datasets is restricted to named NCAP staff through role-based permissions; RCPsych laptops and devices use encryption and automatic time-out security.
- All shared datasets are password protected and contain no direct identifiers. Where required, pseudonymous identifiers may be included so that teams can re-identify their own patients within their clinical systems; NCAP cannot identify individuals from these identifiers. Dataset extracts are checked by a second NCAP staff member prior to release.
- Audit leads may only download pseudonymised patient-level data for their own team via the secure dashboard. These extracts contain no direct identifiers but may include pseudonymous identifiers that allow teams to re-identify their own patients within local clinical systems; NCAP cannot identify individuals from these identifiers.
- Annual review of dataset retention is carried out.
- Deletion requests are issued to Athera Healthcare for any pseudonymised datasets retained on their servers once migration to RCPsych Power BI is complete.
- Clinical Advisors receive only pseudonymised, password-protected extracts and must delete them after use.
- Any identifiable data processed in future for health alerts/outlier analysis would be held on a secure server at the RCPsych, managed under Section 251 approval, and would require a separate DPIA.

Step six: Sign off and record the DPIA outcomes

This step records the approval of the identified data protection risks and outlines the agreed solutions and responsibilities for implementing them.

Risk	Approved solution	Person Responsible and deadline for completion	Approved by
Processing large volumes of pseudonymised mental health data	Data stored in secure RCPsych systems with strict role-based access; pseudonymised only; password protection on all shared files; annual IG review.	Head of IS – completed NCAP Programme manager – completed and ongoing	Head of Audit and Research, CCQI
Storage and processing on third party systems:	GDPR-compliant contract with Athera; secure authentication; migration to RCPsych Power BI; deletion of Athera-held data post-migration.	Head of IS – completed NCAP Programme Manager – completed and ongoing	Head of Audit and Research, CCQI
Email transfer of pseudonymised datasets	All shared datasets are password protected. Datasets containing unique identifiers are only shared with the data source (member organisations). Data emailed are	NCAP team – completed and ongoing	Head of Audit and Research, CCQI

	otherwise made anonymous. No identifiable information will be included in the datasets emailed to sites.		
RCPsych devise loss	Only RCPsych approved laptops are used with appropriate security protections. No identifiable data are stored on laptops.	Head of IS – completed and ongoing	Head of Audit and Research, CCQI
Incorrect dataset shared with a service	All shared datasets are password protected, with a unique password per service. Passwords are not sent with datasets. Emails containing datasets are cross checked by another member of the NCAP team. Identifiable data is not included in datasets sent to sites.	NCAP Programme Manager – completed and ongoing	Head of Audit and Research, CCQI
Unauthorised access by RCPsych staff outside the NCAP team	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	Head of IS - completed	Head of Audit and Research, CCQI

	servers. Only named RCPsych staff have access via remote desktop. All access is logged.		

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

This step outlines how the outcomes of the DPIA are incorporated into the project plan. It identifies the roles responsible for implementing the approved solutions, updating project documentation, and acting as contacts for any future data protection concerns.

Action to be taken	Date for completion of actions	Responsibility for action
NCAP team will request Athera Healthcare, Egress and Microsoft Azure to delete data retained, once no longer required.	Ongoing	NCAP Programme Manager
Contract is in place with Athera Healthcare, Egress and Microsoft Azure who hold appropriate security credentials.	Completed	NCAP Programme Manager
All shared datasets are password protected.	Ongoing	NCAP Programme Manager
Only RCPsych approved laptops are used with appropriate security protections	Completed	Head of IS
Datasets containing unique pseudonymous identifiers are only shared with the originating organisations, identifiable data is not emailed or distributed.	Ongoing	NCAP Programme Manager
Pseudonymous datasets are stored on secure SharePoint	Completed	NCAP Programme Manager

with restricted access to project folders. Computer terminals/ RCPsych laptops time-out and require password access.		
Policy is to review retention of datasets annually.	Ongoing	NCAP Programme Manager
Identifiable data will be stored for the period allowed according to Section 251 approval. Any retention past this date will require further Section 251 approval.	Ongoing	NCAP Programme Manager

Annex 1

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 2

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		x	Not collected or processed by NCAP.
NHS number		x	We have Section 251 approval to receive this identifier for dataset linkage, but it is not currently being used or provided to NCAP
Address		x	Not collected or processed by NCAP.
Postcode		x	We have Section 251 approval to receive this identifier for dataset linkage, but it is not currently being used or provided to NCAP
Date of birth		x	We have Section 251 approval to receive this identifier for dataset linkage, but it is not currently being used or provided to NCAP
Date of death		x	Not collected or processed by NCAP.
Age	x		Age is included to monitor whether differences in care quality or access exist between age groups, supporting the identification of health inequalities. This enables NCAP to highlight variation in outcomes or treatment patterns linked to age and to inform targeted improvement work where disparities are identified.
Sex	x		Sex is collected to monitor whether differences in access, treatment and outcomes exist between males and females. Including this information supports the identification of health inequalities linked to sex and enables NCAP to highlight any variation in care that may require targeted quality improvement
Marital Status		x	Not collected or processed by NCAP.
Gender	x		Gender is collected to assess whether people of different gender identities experience differences in access, experience or outcomes of care. This supports NCAP's ability to identify gender-related health inequalities and to inform improvement work aimed at ensuring equitable care for all service users
Living Habits		X	Not collected or processed by NCAP.
Professional Training / Awards		x	Not collected or processed by NCAP.
Income / Financial / Tax Situation		x	Not collected or processed by NCAP.
Email Address		x	Not collected or processed by NCAP.

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]*
Physical Description		x	Not collected or processed by NCAP.
General Identifier e.g. Hospital No/Paris ID		x	Not collected or processed by NCAP.
Home Phone Number		x	Not collected or processed by NCAP.
Online Identifier e.g. IP Address/Event Logs		x	Not collected or processed by NCAP.
Website Cookies		x	Functional cookies may be used by Athera's online dashboard and from April 2026, by the RCPsych Power BI environment to support general website operation (e.g., authentication and basic functionality). NCAP does not use or process any cookie data, and cookies are not required for NCAP's data collection. No identifiable information is collected through cookies.
Mobile Phone / Device No		x	Not collected or processed by NCAP.
Device Mobile Phone / Device IMEI No		x	Not collected or processed by NCAP.
Location Data (Travel / GPS / GSM Data)		x	Not collected or processed by NCAP.
Device MAC Address (Wireless Network Interface)		x	Not collected or processed by NCAP.
Sensitive Personal Data			
Physical / Mental Health or Condition	x		Specific mental health diagnoses are collected to assess whether treatment offered is concordant with NICE guidelines. Diagnosis is also essential for identifying variation in outcomes, including the impact of multiple conditions, which are associated with poorer clinical trajectories.
Sexual Life / Orientation		X	Not collected or processed by NCAP.
Family / Lifestyle / Social Circumstance	X		Data is collected on whether the person has an identified family member, friend or carer who supports them. This is used to assess whether appropriate family-inclusive interventions and support are being offered in line with NICE guidelines.
Offences Committed / Alleged to have Committed		X	Not collected or processed by NCAP.
Criminal Proceedings / Outcomes / Sentence		X	Not collected or processed by NCAP.
Education / Professional Training	X		Collected alongside employment status to assess whether appropriate education or vocational interventions are being offered in line with NICE guidelines.

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]*
Employment / Career History	x		Employment status is collected to assess the need for education and employment interventions in line with NICE guidelines
Financial Affairs		X	Not collected or processed by NCAP.
Religion or Other Beliefs		X	Not collected or processed by NCAP.
Trade Union membership		X	Not collected or processed by NCAP.
Racial / Ethnic Origin	X		Ethnicity is collected to identify whether differences in access, experience or outcomes exist between different demographic groups. This enables NCAP to detect ethnicity-related health inequalities, highlight variation in care, and inform targeted improvement initiatives where disparities are identified.
Biometric Data (Fingerprints / Facial Recognition)		X	Not collected or processed by NCAP.
Genetic Data		X	Not collected or processed by NCAP.
Use of Mental Health Legislation/DoLS etc.		X	Not collected or processed by NCAP.
Care Data including interventions, procedures, surgery etc.	x		Medication and psychological therapies.
Spare		x	Not collected or processed by NCAP.