Data Protection Impact Assessment

for

National Clinical Audit of Psychosis (NCAP) 2023 bespoke data audit

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, pseudonymous data.
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 – Trusts/organisations and Health Boards will be asked to provide data on care.
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Yes – Trusts/organisations and Health Boards will be asked to provide data on care via an online tool provided by a third-party supplier (SNAP surveys).
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 will be analysed to provide national and regional benchmarking.
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? *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 – Data collected will be pseudonymous and include sensitive data relevant to an individual's care under mental health services including gender, ethnicity, psychological

	and other interventions and physical health assessment and intervention.
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 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 - data will be collected on people with mental health difficulties (including those who lack capacity to consent to care) and will include the elderly, young people aged under 18 years old, and others who may be unable to consent (e.g., those with learning disabilities and other vulnerable groups).
10. Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	Yes - Data is collected via NHS Trusts/Health Boards in Wales and Healthcare Organisations in Ireland. Mental Health Services Dataset (MHSDS) data from England will also be collected from NHS Digital. Privacy notice and opt out information will be available on our website.

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 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). The programme is funded by NHS England and Improvement and the Welsh Government. NCAP aims to improve the quality of care that NHS Mental Health Trusts in England and Health Boards in Wales provide to people with psychosis. Services are measured against criteria relating to the care and treatment they provide, so that the quality of care can be improved.

NCAP has been running since 2017 and was developed to follow on from the National Audit of Schizophrenia (NAS) which took place between 2011-2014. In 2017/18 the audit looked at care being provided to people with psychosis by inpatient and outpatient services. Then from 2018 onwards the audit focused on the quality of care provided by Early Intervention in Psychosis (EIP) teams. These are specialised services providing prompt assessment and evidence-based treatments to people with first-episode psychosis. NCAP has received funding for a further three years up until 31 July 2025 and will continue to focus on healthcare improvement of EIP services.

For the current programme running from 2022-2025 the audit will move away from collecting bespoke audit data and will instead use routine data (e.g., MHSDS in England) which will reduce the burden of data collection on EIP teams and allow them to focus resources on patient care.. The first year of this programme will be a developmental year during which we set up the new audit methodology and pilot it with a few teams prior to rolling it out nationally.

In addition to this NHS England have advised that the new contract for the NCAP would not offer their Mental Health Policy Team sufficient information to assess psychosis services against the NHS Long Term Plan. They therefore proposed and would like to fund at least one further round (one year) of the bespoke data collection audit. This will take place in early 2023.

For all aspects of the audits, participating services will be able to compare their performance with national standards and benchmark their performance against other services.

For the additional bespoke audit in 2023, the audit will not be collecting any patient identifiable information. This DPIA is for the bespoke audit only. Please see our website for the routine data audit DPIA.

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.

Audit of Practice Dataset (Core Audit)	
Data source	Submission from Trust/organisation via online form.
Output	Online dashboard (national, local, and regional level data)
Data shared with	Clinical Advisors – pseudonymous password protected datasets may be shared for data analysis purposes.
Contains identifiable personal information?	Yes – pseudonymised, identification only possible by submitting Trust/organisation.
Contains sensitive information?	Yes (see details below in Annex 4)
Electronic Storage	Pseudonymous data will be stored on RCPsych SharePoint (with restricted access) Net Solving Limited collects submitted forms and creates pseudonymous datasets for export (accessible only with username and password) Pseudonymous dataset may be stored on Clinical Advisor laptop (file is password protected)
Paper/Hard copy storage	No
Comments	

Communications Mailing List	
Data source	Individual request, service contact mapping exercise (online information)
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	

Registered Trust/Organisation Audit Contacts	
Data source	Submission from Trust/organisation via registration form. Minor amendments via email occasionally.
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'.

- Discussed College IG policy and data management processes with project team
- Discussed GDPR requirements with internal Data Protection team and GDPR leads
- Discussed secure storage for identifiable data with IT team

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
Sensitive, pseudonymous data are collected on thousands of service users which are transferred by secure IP transfer from Net Solving Ltd to the SharePoint server	Personal and 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, 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 (Net Solving)	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.
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 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.

Pseudonymous data (electronic) accessed by unauthorised staff at RCPsych	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.
Pseudonymous datasets shared by email	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, if lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.
Laptop containing pseudonymous data that is lost or stolen	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
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.

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).

- Delete data held on third party servers (Net Solving) when no longer required.
- All datasets shared by email are password protected. Checking procedure in place within team for all datasets sent out.
- RCPsych approved laptops are used with appropriate security protections.
- Restricted access to pseudonymous datasets on Sharepoint. Only named staff have access to these.
- Review retention of datasets annually.

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
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. Policy is to review retention of datasets annually. After being held for 5 years, pseudonymous data will be made anonymous by deletion of unique patient identifiers.	Head of IT – completed NCAP Programme manager – completed and ongoing	Dr Alan Quirk, Head of Clinical Audit and Research
Sensitive data held on third party servers (Net Solving Ltd)	Only RCPsych staff have access to the raw data on Net Solving Ltd. Teams will have access to their own pseudonymous data using a secure username and password. All other data available to teams will be aggregated. The NCAP team will request data are	NCAP Programme Manager – completed and ongoing Head of IT – completed	Dr Alan Quirk, Head of Clinical Audit and Research

	deleted from Net Solving Ltd servers once no longer required. Contract is in place with Net Solving Ltd, who hold appropriate security credentials.		
Datasets shared by email	All shared datasets are password protected.	NCAP team – completed and ongoing	Dr Alan Quirk, Head of Clinical Audit and Research
Laptop containing pseudonymous data that is lost or stolen	Only RCPsych approved laptops are used with appropriate security protections.	Head of IT – completed and ongoing	Dr Alan Quirk, Head of Clinical Audit and Research
The wrong datasets are shared with members, containing data on service users from other organisations	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.	NCAP Programme Manager – completed and ongoing	Dr Alan Quirk, Head of Clinical Audit and Research
Pseudonymous data (electronic) 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.	Head of IT - completed	Dr Alan Quirk, Head of Clinical Audit 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**
Online forms are designed with restricted fields to reduce errors.	Completed	NCAP Programme Manager
NCAP team will request Net Solving delete data retained, once no longer required.	Ongoing	NCAP Programme Manager
Contract is in place with Net Solving 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 IT
Pseudonymous datasets are stored on secure SharePoint with restricted access to project folders. Computer terminals/ RCPsych laptops time-out and require password access.	Completed	NCAP Programme Manager
Policy is to review retention of datasets annually.	Ongoing	NCAP Programme Manager
After being held for 5 years, pseudonymous data will be made anonymous by deletion of unique patient identifiers.	Ongoing	NCAP Programme Manager

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?

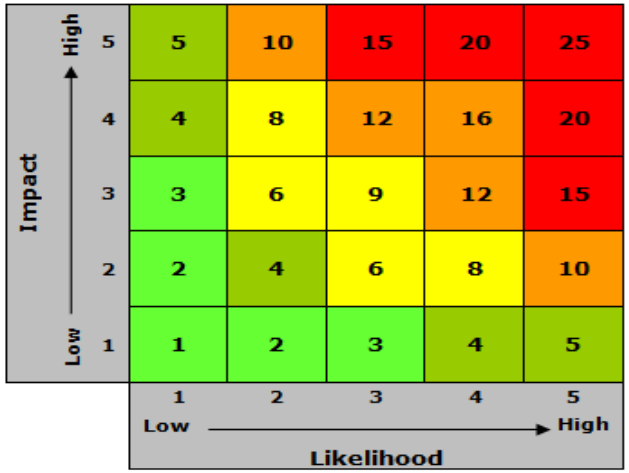
b) What training and instructions are necessary to ensure that staff know how to operate a new system securely?

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		x	
NHS number		x	
Address		x	
Postcode		x	
Date of birth		x	
Date of death		x	
Age	x		There is evidence that service users with some demographic characteristics are more likely to receive some types of care. The aim of including this information is to identify whether some demographic groups receive better/worse care on average and support the develop of change initiatives/local improvement work to address differences where they do exist.
Sex		x	
Marital Status		x	
Gender	x		There is evidence that service users with some demographic characteristics are more likely to receive some types of care. The aim of including this information is to identify whether some demographic groups receive better/worse care on average and support the develop of change initiatives/local improvement work to address differences where they do exist.
Living Habits		X	
Professional Training / Awards		x	
Income / Financial / Tax Situation		x	
Email Address		x	
Physical Description		x	
General Identifier e.g. Hospital No/Paris ID		x	
Home Phone Number		x	
Online Identifier e.g. IP Address/Event Logs		x	
Website Cookies	x		Net Solving Limited uses cookies to indicate previous responses to some types of survey (for example use of usernames) and enhance the functionality of the tools.

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]*
Mobile Phone / Device No		x	
Device Mobile Phone / Device IMEI No		x	
Location Data (Travel / GPS / GSM Data)		x	
Device MAC Address (Wireless Network Interface)		x	
Sensitive Personal Data			
Physical / Mental Health or Condition	x		Specific diagnoses are collected to assess whether treatment offered is concordant with NICE guidelines. Multiple conditions/diagnosis is associated with poorer outcomes.
Sexual Life / Orientation		X	
Family / Lifestyle / Social Circumstance		X	
Offences Committed / Alleged to have Committed		X	
Criminal Proceedings / Outcomes / Sentence		X	
Education / Professional Training	X		Collected alongside employment status. Collected to assess whether appropriate interventions/support is being offered to the person in line with NICE guidelines.
Employment / Career History	x		Employment status is collected in order to assess the need for an education and employment intervention, and to match to data provided by NHS Digital.
Financial Affairs		X	
Religion or Other Beliefs		X	
Trade Union membership		X	
Racial / Ethnic Origin	X		There is evidence that service users with some demographic characteristics are more likely to receive some types of care. The aim of including this information is to identify whether some demographic groups receive better/worse care on average and support the develop of change initiatives/local improvement work to address differences where they do exist.
Biometric Data (Fingerprints / Facial Recognition)		X	
Genetic Data		X	
Use of Mental Health Legislation/DoLS etc.		X	
Care Data including interventions, procedures, surgery etc.	x		Medication and psychological therapies.
Spare		x	