RC PSYCH
ROYAL COLLEGE OF PSYCHIATRISTS

Data Protection Impact Assessment for National Clinical Audit of Psychosis Physical Health and Employment Spotlight Audit 2020/21

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 is being given to you, or you want to use an existing store of data in a different way; you must now consider completing a *Data Protection Impact Assessment* (DPIA). The sort of personal data which will attract a DPIA are: pseudonymised, special category (sensitive), healthcare, social care, financial (this list is not exhaustive). For more information on anonymisation/pseudonymisation please see the references section at the end of this document.

This document comprises two sections:

1. A set of screening questions, for people who are unsure whether or not they need to fill in a DPIA
2. A template form for a DPIA, based on guidance issued by the Information Commissioner's Office (ICO). This form walks you through all the issues you need to consider when conducting a PIA

Please read and complete the DPIA alongside Annex 2 which includes the Data Processing Principles from the GDPR.

Section 1: Screening questions

These questions are intended to help you decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise. You should consider completing a DPIA for projects which are already running where the screening questions can be applied. You can expand on your answers as the project develops if you need to:

1. **Will/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 health data.
2. **Will/does the project compel individuals to provide information about themselves or ask others to disclose it on their behalf? (e.g. 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 (Formic Solutions).
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 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 can 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 – pseudonymous data will be collected and include sensitive information related to an individual's care under mental health services including gender, ethnicity,

For example, health records, criminal records or other information that people would consider to be private. Or any of the sensitive personal data, that is, ethnicity or racial origin, political beliefs, religious beliefs, trade union membership, sexual life.	employment status 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, patients and cases where there is an imbalance in the relationship between the position of the individual and the controller.	Yes - data will be collected on people with mental health difficulties (including those who lack capacity to consent to care) and will include adults and young people over the age of 16 years and the elderly 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 England and Wales. A 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, 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 a three-year improvement programme with a two-year extension which aims to increase the quality of care that NHS Mental Health Trusts in England and Health Boards in Wales provide to people with psychosis. Commissioned by the Healthcare Quality Improvement Partnership on behalf of NHS England, NCAP is the next phase in the development of the National Audit of Schizophrenia. The audit aims to provide those who commission, deliver and use services for people with psychosis with high quality data on the process and outcomes of NHS care.

In years 2, 3 and 4 of the audit, NCAP has examined the quality of care provided by Early Intervention in Psychosis (EIP) teams. The audit measures provision of EIP care against standards based on the Early Intervention in Psychosis Access and Waiting Time standard. Key areas of performance will include the assessment and relevant interventions for physical health and psychological and other interventions (clozapine, supported employment or education programme).

In year 4 (2020/2021), we will also be looking at care received by adults 16 years and older in the community (excluding CAMHS and EIP teams) with a range of psychotic disorders. The spotlight audit of adult community services will assess education and physical health screening and interventions.

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.

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows – where you are getting the data from, where it will be stored and where it could be transferred to. You should also say how many individuals are likely to be affected by the project. Please ensure you identify the Data Controller and Data Processor/s within the flows and any sub-contracted parties.

	Communications Mailing List	Registered Trust/Organisation Audit Contacts	Audit of Practice Dataset
Data source	Individual request, service contact mapping exercise (online information)	Submission from Trust/organisation via registration form. Minor amendments via email occasionally.	Submission from Trust/organisation via online form. Minor amendments will be done during data cleaning via email
Output	Correspondence (emails, letters)	Correspondence (emails, letters)	Reports (National)
Data shared with	N/A	N/A	StatsConsultancy – external statistician may be sent anonymised sections of data for analysis Clinical Advisor – may be shared for data analysis purposes. (pseudonymous dataset only, password protected)
Contains identifiable personal information?	Yes	Yes	Yes – pseudonymised (identification only possible by submitting Trust/ organisation)

Contains sensitive information?	No	No	Yes (see details below in section Justification for collecting personal data)
Electronic Storage	Yes On RCPsych SharePoint (with restricted access)	Yes On RCPsych SharePoint (with restricted access) Formic collects submitted forms (accessible only with username and password)	Yes Pseudonymous data will be stored on RCPsych SharePoint (with restricted access) Formic collects submitted forms (accessible only with username and password) Pseudonymous dataset may be stored on Clinical Advisor laptop (file is password protected)
Paper/Hard copy storage	No	No	No
Comments			

Datasets are downloaded and stored on the internal drives once reports have been published. Registration and communications contacts are stored for the life of the audit (unless subject requests erasure), please see our clinical audit privacy notice for more information. On closure of project HQIP requirements will be followed. Pseudonymous data are stored for the life of the audit plus 5 years as per guidance on restricted access SharePoint.

Requests for data from the audit will go through the HQIP Data Access Request Group (DARG) as per HQIP guidance.

Step 3: Consultation requirements

Explain what practical steps you will take to ensure that 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.

e.g. 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
- Provide evidence of GDPR compliance to commissioning body, Healthcare Quality Improvement Partnership, via contract management meetings

Step three: 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.

Annex 2 can be used to help you identify the DPA related compliance risks.

Privacy issue	***Risk to individuals***	***Compliance risk***	***Associated organisation / corporate risk***
Sensitive data are collected on thousands of service users which are transferred by secure IP transfer from Formic 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 data held on third party servers (Formic Solutions)	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 is stored on thousands of service users, which is copied across software files for cleaning/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 or printed) 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 four: Identify solutions

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

Risk: use the Corporate Risk Matrix to calculate a score based on likelihood and impact (Annex 3)	***Solution(s)***	***Result:*** *is the risk eliminated, reduced, or accepted?*	***Evaluation:*** *is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?*
1. Sensitive data held on third party servers (Formic Solutions) **Risk score: 8**	NCAP team is able to use Formic's online system to delete data retained, once no longer required. Contract is in place with Formic who appropriate hold security credentials. Formic previously held an Information Governance Statement of Compliance (IG SoC) Level 2 and has submitted a Data Security and Protection Toolkit for 2019. Formic is ISO27001:2013 certified and hold Cyber Essentials Plus.	**Risk is reduced**	**Impact is justified:** Third party supplier is required for the specialised IT system and management of large data submissions, and secure storage of identifiable information.
2. Datasets shared by email **Risk score: 8**	All shared datasets are password protected.	**Risk is reduced**	**Impact is justified:** Datasets are emailed to

	Datasets containing unique identifiers are shared with the data source (participating services). Data emailed are otherwise made anonymous.		members for essential data cleaning and local analysis.
3. Laptop containing pseudonymous data that is lost or stolen **Risk score: 6**	Only RCPsych approved laptops are used with appropriate security protections.	**Risk is reduced**	**Impact is justified:** Storage and use of data on laptops supports project workflow.
4. The wrong datasets are shared with members, containing data on service users from other organisations **Risk score: 6**	All shared datasets are password protected; no identifiable data are returned to sites. Checking procedure in place within team for all datasets sent out.	**Risk is reduced**	**Impact is justified:** Datasets are emailed to members for essential data amendments and local analysis.
5. Data (electronic or printed, pseudonymous) accessed by unauthorised staff at RCPsych **Risk score: 4**	Pseudonymous datasets are stored on secure SharePoint with restricted access to project folders. Computer terminals time-out and require password access.	**Risk is reduced**	**Impact is justified:** Extent of staff access to data stored electronically is the minimum necessary for the delivery of project aims.
6. Pseudonymous data collected is retained for five years. **Risk score: 4**	Policy is to review retention of datasets annually. After being held for 5 years, pseudonymous data will be made anonymous by	**Risk is reduced**	**Impact is justified**: Pseudonymous data are retained to ensure resolution of queries. Validity of reporting. Copying datasets is essential for the stages of

	deletion of unique patient identifiers. Datasets are stored on secure SharePoint with restricted access.		data cleaning, analysis

Step five: 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 held on third party servers (Formic Solutions)	The NCAP team will request data are deleted from Formic servers, once no longer required.	Ella Webster, Programme Mgr. Completed and ongoing activity	Alan Quirk, Head of Audits and Research.
	Contract is in place with Formic, who hold appropriate security credentials.	Phil Burke, Head of IT Completed	Alan Quirk, Head of Audits and Research.
	Only named RCPsych staff will have access to the NCAP data on Formic servers. All access is logged by Formic.	Ella Webster, Programme Mgr. Completed and ongoing activity	Alan Quirk, Head of Audits and Research.
Datasets shared by email	All shared datasets are password protected.	Ella Webster, Programme Mgr. Completed and ongoing activity	Alan Quirk, Head of Audits and Research.
	Datasets containing unique identifiers are only shared with the data source (member organisations). Data emailed are otherwise made anonymous.	Ella Webster, Programme Mgr. Completed and ongoing activity	Alan Quirk, Head of Audits and Research.
Laptop containing pseudonymous data that is lost or stolen	Only RCPsych approved laptops are used with appropriate security protections.	Ella Webster, Programme Mgr. Completed and ongoing activity	Alan Quirk, Head of Audits 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.	Ella Webster, Programme Mgr. Completed and ongoing activity	Alan Quirk, Head of Audits and Research.
Pseudonymous data (electronic or printed) 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.	Phil Burke, Head of IT Completed	Alan Quirk, Head of 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	Policy is to review retention of datasets annually.	Ella Webster, Programme Mgr. Completed and ongoing activity	Alan Quirk, Head of Audits and Research
	After being held for 5 years, pseudonymous data will be made anonymous by deletion of unique patient identifiers.	Ella Webster, Programme Mgr.	Alan Quirk, Head of Audits and Research.
	Pseudonymous datasets are stored on secure SharePoint with restricted access.	Phil Burke, Head of IT Completed	Alan Quirk, Head of Audits and Research.

Step six: 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	Ella Webster
NCAP team will request Formic delete data retained, once no longer required.	Ongoing	Ella Webster
Contract is in place with Formic who hold appropriate security credentials.	Completed	Phil Burke
All shared datasets are password protected.	Completed	Ella Webster
Only RCPsych approved laptops are used with appropriate security protections	Completed	Ella Webster
All shared datasets are password protected.	Ongoing	Ella Webster
Pseudonymous datasets are stored on secure SharePoint with restricted access to project folders. Computer terminals/ RCPsych laptops time-out and require password access.	Completed	Ella Webster
Policy is to review retention of datasets annually.	Ongoing	Ella Webster
After being held for 5 years, pseudonymous data will be made anonymous by deletion of unique patient identifiers.	Ongoing	Ella Webster

Contact point for future privacy concerns
Richa Sharma, Head of Membership Services + Faculties/Acting Company Secretary – Data Protection Officer 020 8618 4086

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 8618 4086

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').**

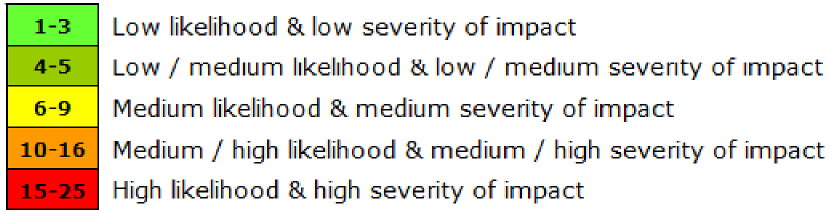
   a) Do any new systems provide protection against the security risks you have identified?

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

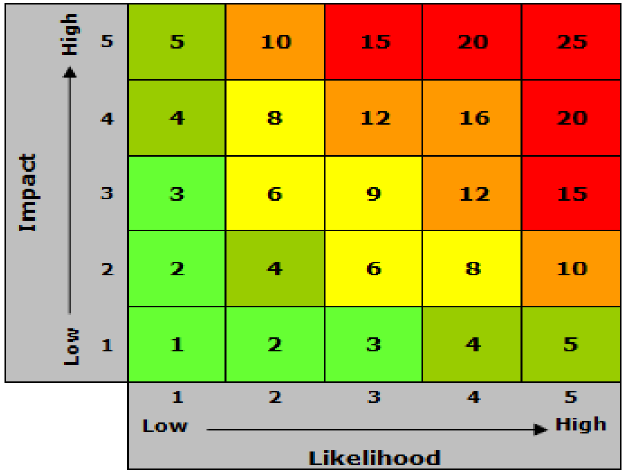
Annex 3

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



High	5	5	10	15	20	25
	4	4	8	12	16	20
Impact	3	3	6	9	12	15
	2	2	4	6	8	10
Low	1	1	2	3	4	5
		1	2	3	4	5
		Low		Likelihood		High

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		✓	
NHS number		✓	
Address		✓	
Postcode		✓	
Date of birth		✓	
Date of death		✓	
Age	✓		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	✓		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.
Marital Status		✓	
Gender	✓		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		✓	
Professional Training / Awards		✓	
Income / Financial / Tax Situation		✓	
Email Address		✓	
Physical Description		✓	
General Identifier e.g. Hospital No/Paris ID		✓	
Home Phone Number		✓	
Online Identifier e.g. IP Address/Event Logs		✓	

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]*
Website Cookies	✓		Formic software uses cookies to indicate previous responses to some types of survey (for example use of usernames) and enhance the functionality of the tools.
Mobile Phone / Device No		✓	
Device Mobile Phone / Device IMEI No		✓	
Location Data (Travel / GPS / GSM Data)		✓	
Device MAC Address (Wireless Network Interface)		✓	
Sensitive Personal Data			
Physical / Mental Health or Condition	✓		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		✓	
Family / Lifestyle / Social Circumstance		✓	
Offences Committed / Alleged to have Committed		✓	
Criminal Proceedings / Outcomes / Sentence		✓	
Education / Professional Training	✓		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	✓		Employment status is collected in order to assess the need for an education and employment intervention.
Financial Affairs		✓	
Religion or Other Beliefs		✓	
Trade Union membership		✓	
Racial / Ethnic Origin	✓		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)		✓	
Genetic Data		✓	
Use of Mental Health Legislation/DoLS etc.		✓	
Care Data including interventions, procedures, surgery etc.		✓	
Spare		✓	