# Data Protection Impact Assessment

The Prescribing Observatory for Mental Health UK (POMH-UK)

February 2021

## Document Information

| | |
|---|---|
| Title of document | Data Protection Impact Assessment |
| Version number | 1.1 |
| Type of document | Template for Assessment |
| 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 | All College staff and contractors |
| Distribution | Intranet (electronic) |
| Consultation | Interim Director of Information Services. GDPR Project Steering Group |
| Approved by | Richa Kataria |
| Date of approval | July 2018 |
| Author | Kathryn Campling GDPR Consultant |
| Review date | Every 2 years or sooner if required |

## Document Control

## Template

| Version Number | Reason for Change | Description of Change | Date of Change | Author |
|---|---|---|---|---|
| Draft | Original draft | Creation | June 2018 | Kathryn Campling GDPR Consultant |
| V1.1 | Amendments to include Table of contents, cover page, document control, tables and risk register annex 3 | Updates | June 2018 | Susie Griffin GDPR Project Manager |

### Project content

| Version number | Reason for Change | Description of Change | Date of Change | Author |
|---|---|---|---|---|
| v1 | n/a | Creation | Nov 2018 | Gavin Herrington, Programme Manager |
| v2 | 2-year review | Amendments to Section 1 Screening Questions, Amendments to Section 2, Data Flow, Summary, Consultation Requirements, Identification of Risks, Solution and implementation. | Feb 2021 | Gavin Herrington, Programme Manager |

# 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 DPIA

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 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 – for the purpose of clinical audit and quality improvement, the project requires participating members (Trusts, specialist mental health services) to provide service user data |
| 3. **Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?** | Yes – pseudonymous data are collected via an online tool provided by a third party supplier (Formic Solutions). In addition, anonymous or aggregated data may be shared with an external consultant for further statistical analysis, or presented to external advisory group members as part of the review and analysis of data |
| 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 recorded as part of the direct care of patients are supplied to POMH-UK in a pseudonymised format for the purpose of clinical audit and quality improvement. |
| 5. **Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.** This would cover things like 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? For example, health records, criminal records or other information that people would consider to be private.**<br>Or any of the sensitive personal data, that is, ethnicity or racial origin, political beliefs, religious beliefs, trade union membership, sexual life. | Yes - sensitive pseudonymous data are collected relevant to an individual's care under mental health services, such as their age, gender, ethnicity, diagnosis, Mental Health Act status, medication, and treatment details |
| **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 – service users under the care of mental health services |
| **10. Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?** | Yes – pseudonymous service user data are collected from the Trusts/ organisations responsible for their care. Only member Trusts/organisations are actively provided with our online privacy notice by POMH-UK (though the POMH-UK privacy notice is publicly available online). POMH-UK does not have direct contact with service users. |

## 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 Prescribing Observatory for Mental Health (POMH-UK) is a subscription based project that helps specialist mental health services across the UK improve their prescribing practice. To achieve this, we develop audit-based Quality Improvement Programmes that focus on specific topics within mental health prescribing, which are priority areas for service user care.

Data are collected locally by participating members from a variety of patient records, which are then supplied to the project via an online data collection tool.

Prescribing practice is measured against recognised, national standards. After analysing the data, members receive a customised report that benchmarks their performance against data collected from other participating Trusts and healthcare organisations. Digital and printed reports are released along with slide-sets to aid the local communication of results. Shortfalls in practice indicated by key national findings lead to the development of change interventions, supporting members' own quality improvement initiatives.

Individual reports and slide-sets contain aggregate data only. Aggregate data may also be published in scientific journals and appear in the public domain. High levels of participation by eligible mental health services across the UK, lends significant weight to the validity of findings and the potency of the data collected.

The data collected are pseudonymous but comprise sensitive information relevant to an individual's care under mental health services (such as age, gender, ethnicity, diagnosis, Mental Health Act status, medication and treatment details). These service user data are provided to the project by Trust/healthcare organisations on their behalf. As we are collecting pseudonymous data as part of a clinical audit for the purpose of quality improvement and patient care, explicit patient authorisation for sharing these data is not required. However, for reasons outlined in section 1, such as the potential privacy concerns of these sensitive data, relating to individuals who may be considered vulnerable, a DPIA is warranted.

## 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.*

***Data flow***

| | |
|---|---|
| Data controller | POMH-UK decides scope of data collection and produces an audit tool. The audit tool is released and data are requested from members |
| | ↓ |
| Data processor and source | Members submit pseudonymous data online using Formic solutions data collection tool |
| | ↓ |
| Data processor | Pseudonymous data are stored on Formic Solutions servers |
| | ↓ |
| Data controller | Pseudonymous data are downloaded by POMH-UK and stored on RCPsych's secure, cloud-based environment (SharePoint) with restricted access. |
| | ↓ |
| Data controller | POMH-UK project team email members portions of their submitted datasets as password protected attachments, to resolve data cleaning queries |
| | ↓ |
| Data controller | Pseudonymous data are accessed online by POMH-UK project team and analysed (by up to 6 people). Data may be displayed on shared screens during video calls with members of the POMH-UK team working remotely. |
| | ↓ |
| Data controller | Pseudonymous data may be downloaded by POMH-UK project team working remotely to their RCPsych issued device or laptop. Downloaded data remains encrypted and within a secure environment. |
| | ↓ |
| Data controller | Limited amounts of the pseudonymous data may be printed and analysed by the project team working on RCPsych premises (up to 6 people). |
| | ↓ |
| Data controller | Any materials printed on RCPsych premises are stored by the project team in locked cabinets/drawers and destroyed in confidential waste bins after use. |
| | ↓ |
| Data processor | Aggregated data may be displayed/presented on screen during video calls or in-person meetings with expert or other advisory group members, external to RCPsych (2 to 3 external members). |

| | |
|---|---|
| | ↓ |
| Data processor | Anonymous data are shared by email with a subcontractor (StatsConsultancy) for statistical analysis of data (1 individual) |
| | ↓ |
| Data processor | Reports containing aggregated data are supplied to a printing company via secure, online file-sharing site. |
| | ↓ |
| Data controller | Aggregated data are published in reports and slides sets and released via password protected member webpages. Member postal addresses may also be shared with an external printing company to complete mailing of printed reports to members. |
| | ↓ |
| Data controller | POMH-UK project team delete datasets from Formic data collection system once reporting has been completed. |
| | ↓ |
| Data controller | Anonymous, aggregated data may appear within papers shared with scientific journals, for publication in the public domain. |
| | ↓ |
| Data controller | Anonymous, aggregated data may be shared with other external groups undertaking collaborative work with POMH-UK on specific topics (e.g. NICE). |
| | ↓ |
| Data processor | BSc students and clinical fellows assigned to the project may have limited access to anonymised datasets on RCPsych secure environment, to support BSc thesis or wider QI initiatives |

***Summary***

| | ***Service user personal and healthcare records*** |
|---|---|
| ***Data source:*** | NHS Trusts and Health Boards (England, Wales, Scotland, Northern Ireland) and other independent, private or charitable mental health services |
| ***Output:*** | Datasets in SPSS and Excel for cleaning and analysis<br>Customised reports and slide-sets (with data at national, Trust and team level) |
| ***Data shared with:*** | Project team (pseudonymous data)<br>Member Trusts/local POMH leads (pseudonymous data)<br>External statistician (anonymous data)<br>BSc students, clinical fellows (anonymous data)<br>Advisory group members (anonymous, aggregated data)<br>Other collaborators, experts (anonymous, aggregated data)<br>Printing company (anonymous, aggregated data) |
| ***Contains identifiable personal information?*** | Yes – datasets contain pseudonymous data. Datasets contain a unique personal identifier that corresponds with additional personal records held by the Trust/healthcare organisation. Used together these data can identify the individual. |
| ***Contains sensitive information?*** | Yes - clinical information related to the individual's care under mental health services |
| ***Electronic Storage:*** | Yes -<br>**RCPsych**. Datasets are held in a secure cloud-based environment, or downloaded to secure environment on RCPsych issued laptops. Data on all RCPsych computers are password protected and encrypted. Access is restricted to specified members of the POMH team. Any datasets shared by email are password protected. Any laptops used to store or transport data are supplied by the College with appropriate security and password protection.<br><br>**Formic solutions** (data entry system). Datasets are held by this third party supplier until deleted by POMH-UK. Formic hold the following security credentials: ISO27001:2013 Certified, Data Security and Protection Tookit: status 19/20 Standards. Cyber Essentials Plus Certified.<br><br>**Statsconsultancy** (statistician). Anonymised datasets only are emailed to this third party for statistical analysis, when required. A data sharing agreement with this third party sets out terms for the secure handling, use and destruction of the data. |
| ***Paper/Hard copy storage:*** | Yes - any materials printed by the POMH team whilst on RCPsych premises are stored in locked cabinets/drawers for as long as necessary for analysis. After use, any printed data are placed in confidential waste bins and securely destroyed. Datasets are not printed by staff working remotely. |
| ***Comments:*** | |

In addition to the sensitive pseudonymous data outlined above, Member contact names, telephone numbers and email addresses are collected for the purpose of administering their membership and for booking delegate places at our regional events. All such contact details are stored on the same secure environment with restricted access.

## 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
- Discussed security of remote working arrangements with IS Team.
- 'Data management' added to project's monthly review meeting agenda for ongoing review by team and joint-heads.
- Data collection tools are shared and discussed with participating Members at our regional events. This affords data suppliers the opportunity to review the purpose and scope of data collection, reducing the risk of accumulating excessive data.

## Step three: Identify the Data Protection and related risks

*Identify the key Data Protection risks and the associated compliance and corporate risks.*

| ***Privacy issue*** | ***Risk to individuals*** | ***Compliance risk*** | ***Associated organisation / corporate risk*** |
|---|---|---|---|
| Sensitive pseudonymous data are collected on thousands of service users for each audit, which is copied across different software for cleaning/ analysis | Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost | Creating multiple copies of datasets are a challenge for effective data management and control. For example, in resolution of Subject Access Requests | Could lead to regulatory fines, reputational damage, decline in membership and funding |
| Personally identifiable service user data (e.g. NHS number, full date of birth) may be mistakenly shared by Trusts during data collection | Sensitive data relating to an individual's mental health is linked to identifying data, which could cause harm or distress if shared | The project could receive personal, excessive data without purpose or appropriate controls/ permissions. The impact of any data breach is increased | Could lead to regulatory fines, reputational damage, decline in membership and funding |
| Pseudonymous data (electronic or printed) accessed by unauthorised staff at RCPsych, or by others externally whilst staff work remotely. | Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost | Data 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, decline in membership and funding |
| Pseudonymous 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 is 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, decline in membership and funding |
| Datasets shared by email | Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost | Data is subject to unlawful access or processing, if lost or shared as part of a data breach | Could lead to regulatory fines, reputational damage, decline in membership and funding |
| A laptop containing pseudonymous data is lost or stolen | Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost | Data 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, decline in membership and funding |

| | | | |
|---|---|---|---|
| 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 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, decline in membership and funding |
| Staff working remotely access data on their personal laptops/computers without RCPsych security controls | Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost | Data 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, decline in membership and funding |

## 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?* |
|---|---|---|---|
| Personally identifiable service user data (e.g. NHS number, full date of birth) may be mistakenly shared by Trusts during data collection<br>**Risk score: 8** | Data collection forms include clear warnings against supplying excessive and unnecessary personal data.<br>Online forms are designed with restricted fields to reduce errors. | **Risk is reduced** | **Impact is justified:**<br>Opportunities to submit unwanted data are reduced but still exist, due to 'free text' fields. These are necessary for the accuracy and completeness of reporting. |
| Pseudonymous data held on third party servers (Formic Solutions)<br>**Risk score: 8** | POMH is able to use Formic's online system to delete data retained, once no longer required.<br>A contract is in place with Formic, who hold appropriate security credentials: (ISO27001:2013 Certified, Cyber Essentials Plus Certified, IGSoC (IG Toolkit) level 2 attainment) | **Risk is reduced** | **Impact is justified:**<br>Third party supplier is required for the specialised IT system and management of large data submissions |
| Datasets shared by email<br>**Risk score: 8** | All shared datasets are password protected.<br>Datasets containing unique identifiers are only shared with the data source (member organisations). Data emailed are otherwise made anonymous. | **Risk is reduced** | **Impact is justified:**<br>Datasets are emailed to members for essential data cleaning and local analysis.<br>Datasets emailed to the statistician are necessary for complete analysis. |

| | | | |
|---|---|---|---|
| A laptop containing pseudonymous data is lost or stolen<br>**Risk score: 6** | Only college approved laptops are used with appropriate security protections | **Risk is reduced** | **Impact is justified:**<br>Storage and use of data on laptops supports project workflow. |
| Staff working remotely access data on their personal laptops/computers, without RCPsych security controls<br>**Risk score: 6** | POMH team working remotely are all issued with RCPsych laptops, with appropriate security protections. Downloaded data remain within a secure environment. Use of personal computers is not permitted. | **Risk is reduced** | **Impact is justified:**<br>Staff are currently required to work from home. Remote access to data is essential. |
| Pseudonymous data (electronic or printed) accessed by unauthorised staff at RCPsych, or by others externally, whilst staff work remotely.<br>**Risk score: 4** | Datasets are stored in a secure cloud-based environment with restricted access to project folders. RCPsych computer terminals and laptops time-out and require password access.<br>Data printed at RCPsych exclude unique patient identifiers, are stored in locked cabinets and are securely destroyed after use. Datasets are not printed by staff working remotely. | **Risk is reduced** | **Impact is justified:**<br>Staff are currently required to work from home. Remote access to data is essential.<br>Print-outs support necessary analysis/ discussion and contain anonymous data only. |
| Sensitive pseudonymous data are collected on thousands of service users for each audit, which is copied across software files retained indefinitely for long-term statistical analysis<br>**Risk score: 4** | Policy is to review retention of datasets annually.<br>After being held for 5 years, pseudonymous data will be made anonymous by deletion of unique patient identifiers.<br>Datasets are stored in a secure cloud-based environment with restricted access. | **Risk is reduced** | **Impact is justified**:<br>Pseudonymous data are retained to ensure resolution of queries and for purpose of long-term statistical analysis and benchmarking. The volume of data collection is essential for the purpose of the project and validity of reporting. Copying datasets is essential for the stages of data cleaning, analysis and production of reports. |

## 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 |
|---|---|---|---|
| *Personally identifiable service user data (e.g. NHS number, full date of birth) may be mistakenly shared by Trusts during data collection* | Data collection forms include clear warnings against supplying excessive and unnecessary personal data. | Gavin Herrington, Programme Mgr.<br>*Completed* | Alan Quirk, Head of Audit and Research |
| | Online forms are designed with restricted fields to reduce errors. | Gavin Herrington, Programme Mgr.<br>*Completed and ongoing activity* | Alan Quirk, Head of Audit and Research |
| *Pseudonymous data held on third party servers (Formic Solutions)* | POMH is able to use Formic's online system to delete data retained, once no longer required. | Gavin Herrington, Programme Mgr.<br>*Completed and ongoing activity* | Alan Quirk, Head of Audit and Research |
| | A contract is in place with Formic, who appropriate hold security credentials. | Phil Burke, Director of IS<br>*Completed* | Alan Quirk, Head of Audit and Research |
| *Datasets shared by email* | All shared datasets are password protected. | Gavin Herrington, Programme Mgr.<br>*Completed* | Alan Quirk, Head of Audit and Research |
| | Datasets containing unique identifiers are only shared with the data source (member organisations). Data emailed are otherwise made anonymous. | Gavin Herrington, Programme Mgr.<br>*Completed and ongoing activity* | Alan Quirk, Head of Audit and Research |
| *Laptop containing pseudonymous data is lost or stolen* | Only college approved laptops are used with appropriate security protections | Gavin Herrington, Programme Mgr.<br>*Completed and ongoing activity* | Alan Quirk, Head of Audit and Research |

| | | | |
|---|---|---|---|
| *Staff working remotely access data on their personal laptops/computers, without RCPsych security controls* | POMH team working remotely are all issued with RCPsych laptops, with appropriate security protections. Downloaded data remain within a secure environment. Use of personal computers is not permitted. | Gavin Herrington, Programme Mgr.<br>*Completed and ongoing activity* | Alan Quirk, Head of Audit and Research |
| *Pseudonymous data (electronic or printed) accessed by unauthorised staff at RCPsych or by others externally, whilst staff work remotely.* | Datasets are in a secure cloud-based environment with restricted access to project folders. RCPsych computer terminals and laptops time-out and require password access. | Phil Burke, Director of IS<br>*Completed* | Alan Quirk, Head of Audit and Research |
| | Data printed at RCPsych exclude unique patient identifiers, are stored in locked cabinets and are securely destroyed after use. Datasets are not printed by staff working remotely. | Gavin Herrington, Programme Mgr.<br>*Completed and ongoing activity* | Alan Quirk, Head of Audit and Research |
| *Sensitive pseudonymous data are collected on thousands of service users for each audit, which is copied across software files retained indefinitely for long-term statistical analysis* | After being held for 5 years, pseudonymous data will be made anonymous by deletion of unique patient identifiers. | Gavin Herrington, Programme Mgr.<br>*Ongoing activity* | Alan Quirk, Head of Audit and Research |
| | Datasets are stored in a secure cloud-based environment with restricted access. | Phil Burke, Director of IS<br>Completed | Alan Quirk, Head of Audit 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** |
|---|---|---|
| Data collection forms include clear warnings against supplying excessive and unnecessary personal data. | Completed | Gavin Herrington, Programme Manager |
| Online forms are designed with restricted fields to reduce errors. | Completed for current forms.<br>Ongoing - review and testing of future forms required for each QIP topic by POMH team, prior to public release. | Gavin Herrington, Programme Manager |
| POMH is able to use Formic's online system to delete data retained, once no longer required. | Completed for redundant datasets.<br>Ongoing - review and deletion of future datasets required for each QIP topic by the POMH team, after data entry period ends. | Gavin Herrington, Programme Manager |
| Contract is in place with Formic, who appropriate hold security credentials. | Completed. | Gavin Herrington, Programme Manager |
| All shared datasets are password protected. | Completed.<br>Ongoing – passwords to be set for datasets for all future QIP topics, when created. | Gavin Herrington, Programme Manager |
| Datasets containing unique identifiers are only shared with the data source (member organisations). Data emailed are otherwise made anonymous. | Completed for current communications<br>Ongoing - as per requirements for data cleaning and analysis for QIP topics. | Gavin Herrington, Programme Manager |
| Only college approved laptops are used with appropriate security protections | Completed. | Gavin Herrington, Programme Manager |

| | | |
|---|---|---|
| POMH team working remotely are all issued with RCPsych laptops, with appropriate security protections. Downloaded data remain within a secure environment. Use of personal computers is not permitted. | Completed for current team.<br>Ongoing – change of staff will require collection and redistribution of laptops plus training, for those working remotely | Gavin Herrington, Programme Manager |
| Datasets are in a secure cloud-based environment with restricted access to project folders. RCPsych computer terminals and laptops time-out and require password access. | Completed. | Gavin Herrington, Programme Manager |
| Data printed at RCPsych exclude unique patient identifiers, are stored in locked cabinets and are securely destroyed after use. Datasets are not printed by staff working remotely. | Completed for current materials.<br>Ongoing – required practice for all future QIP topics, as materials are produced. | Gavin Herrington Programme Manager |
| After being held for 5 years, pseudonymous data will be made anonymous by deletion of unique patient identifiers. | Ongoing/continuous requirement | Gavin Herrington, Programme Manager |
| Datasets are stored in a secure cloud-based environment with restricted access. | Completed. | Gavin Herrington, Programme Manager |

| **Contact point for future privacy concerns** |
|---|
| Data Protection team: DataProtection@rcpsych.ac.uk |

# Annex 1

## Primary contact for advice and guidance

Data Protection Officer
DataProtection@rcpsych.ac.uk
Royal College of Psychiatrists
21 Prescot Street
London
E1 8BB

# 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?

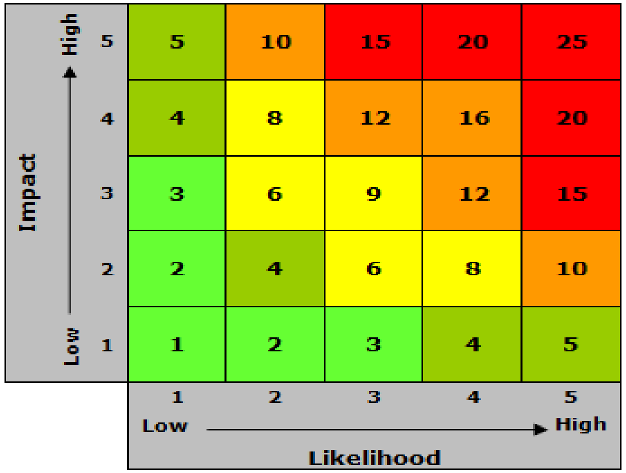
    b) What training and instructions are necessary to ensure that staff know how to operate a new system securely?

# 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 |



| Impact | | | | | | |
|---|---|---|---|---|---|---|
| High | 5 | 5 | 10 | 15 | 20 | 25 |
| | 4 | 4 | 8 | 12 | 16 | 20 |
| | 3 | 3 | 6 | 9 | 12 | 15 |
| | 2 | 2 | 4 | 6 | 8 | 10 |
| Low | 1 | 1 | 2 | 3 | 4 | 5 |
| | | 1<br>Low | 2 | 3 | 4 | 5<br>High |
| | | Likelihood | | | | |

# 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 | ✓ | | Demographic data to inform analysis and quality improvement |
| Sex | ✓ | | Demographic data to inform analysis and quality improvement |
| Marital Status | | ✓ | |
| Gender | ✓ | | Demographic data to inform analysis and quality improvement |
| 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 | | ✓ | |
| Website Cookies | | ✓ | |
| 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 | ✓ | | |
| Sexual Life / Orientation | | ✓ | |
| Family / Lifestyle / Social Circumstance | | ✓ | |
| Offences Committed / Alleged to have Committed | | ✓ | |

| **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]* |
|---|---|---|---|
| Criminal Proceedings / Outcomes / Sentence | | ✓ | |
| Education / Professional Training | | ✓ | |
| Employment / Career History | | ✓ | |
| Financial Affairs | | ✓ | |
| Religion or Other Beliefs | | ✓ | |
| Trade Union membership | | ✓ | |
| Racial / Ethnic Origin | ✓ | | Demographic data to inform analysis and quality improvement |
| Biometric Data (Fingerprints / Facial Recognition) | | ✓ | |
| Genetic Data | | ✓ | |
| Use of Mental Health Legislation/DoLS etc. | ✓ | | Clinical data to inform analysis and quality improvement |
| Care Data including interventions, procedures, surgery etc. | ✓ | | Clinical data to inform analysis and quality improvement |