**Data Protection Impact Assessment**

**Severe Mental Illness and Learning Disability Annual Physical Health Checks – ‘Super Team’**

**Version 5**

Data Protection Impact Assessment

|  |  |
| --- | --- |
| **Project:** | Severe Mental Illness and Learning Disability Physical Health Checks – ‘Super Team’ |
| **Date of Creation:** | 01/02/2021 |
| **Date of Review:** | 23/07/2021 |
| **Version:** | 5 |
| **Author:** | Dr Georgina Ruddle |
| **Information Asset Owner:** | <practice to insert name of responsible individual> |

|  |  |
| --- | --- |
| **Data Protection Officer Sign Off** | |
| **Mandatory DPIA?** | Yes |
| **ICO Notification Required?** | No |
| **Data Subject Notification Required?** | No |
| **Add to Practice Record of Processing?** | Yes |
| **Add to Practice Risk Register?** | No |
| **Approved By:** | Jason Roberts (DPO) |
| **Approved Date:** | 23/07/2021 |

## Amendments Summary

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date Issued** | **Section** | **Subject** |
| 1 | 4/02/2021 | NA | First version of DPIA completed |
| 2 | 11/02/2021 | 4.2 | Updated to include LD and inclusion of CCG team |
| 3 | 24/02/2021 | 4.2 | Updated following feedback from CSU\CCG |
| 4 | 11/06/2021 | 4.2 & 9 | Updated to reflect that FOHC will be producing and sending initial correspondence to patients. |
| 5 | 23/07/2021 | 4.2 | Updated to include detail around Bath Mind and Swindon & Gloucestershire Mind supporting FOHC. |

Contents

[Amendments Summary 3](#_Toc74560471)

[1. Introduction 4](#_Toc74560472)

[2. Screening Questions 4](#_Toc74560473)

[3. Identify the need for a DPIA 5](#_Toc74560474)

[4. Description of the Data Processing 6](#_Toc74560475)

[5. Assessment of Necessity and Proportionality 8](#_Toc74560476)

[6. Assessment of Risks to Data Subjects 9](#_Toc74560477)

[7. Measures to Address Risks to Data Subjects 9](#_Toc74560478)

[8. Prior Consultation 10](#_Toc74560479)

[9. Association with the GDPR principles 10](#_Toc74560480)

[10. DPO Recommendations 13](#_Toc74560481)

# Introduction

* 1. Data Protection Impact Assessments (DPIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals’ expectations of their rights as a data subject under the GDPR. An effective DPIA will allow organisations to identify and resolve problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.
  2. This DPIA is based on the guidance documents provided by the Information Commissioners Office (ICO) to support the data protection by design approach and the information captured will ensure reasonable steps are taken during the implementation of any new system or process.

# Screening Questions

* 1. The GDPR requires that a DPIA is mandatory if the processing is likely to result in a high risk to the rights and freedoms of natural persons. The following screening questions will identify if the processing is likely to result in a high risk:

|  |  |  |
| --- | --- | --- |
| **No.** | **Mandatory DPIA Screening Question** | **Yes or No** |
| M1 | Will the project make use of a new technology (system) to process personal or special category data? | no |
| M2 | Will the project involve systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals? | no |
| M3 | Will the project involve the large scale processing of special categories of personal data? | yes |
| M4 | Will the project involve the large scale, systematic monitoring of public areas (CCTV)? | no |

*If any of the above questions have been answered as “Yes”, than it is a mandatory requirement to complete a DPIA.*

* 1. This table defines a selection of additional screening questions which will help to understand if a DPIA is recommended best practice.

|  |  |  |
| --- | --- | --- |
| **No.** | **Recommended DPIA Screening Question** | **Yes or No** |
| R1 | Will the project involve the collection of new information about individuals? | yes |
| R2 | Will the project compel individuals to provide information about themselves? | no |
| R3 | Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? | yes |
| R4 | Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? | no |
| R5 | Will the project require you to contact individuals in ways that they may find intrusive? | no |
| R6 | Will the project involve monitoring of staff via CCTV? | no |

*If there are two or more “Yes” answers, it is appropriate to complete a DPIA.*

# Identify the need for a DPIA

* 1. The need for a DPIA has been identified as a result of the following screening questions:

|  |  |
| --- | --- |
| **No.** | **Details** |
| M3 | Will the project involve the large scale processing of special categories of personal data? |
| R1 | Will the project involve the collection of new information about individuals? |
| R3 | Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? |

# Description of the Data Processing

* 1. Details of the personal data to be processed:

|  |  |
| --- | --- |
| **Question** | **Answer** |
| What categories of personal data will be processed? | Name, Address, DOB, NHS number, telephone numbers. |
| What categories of special category data will be processed? | Data concerning health |
| What are the categories of data subject whose personal data will be processed? | Patients  Vulnerable adults |
| What is the purpose of the data processing?  (Why is the data being processed?) | To allow First Option Healthcare to book and complete health checks for cohorts of vulnerable patients. |
| Are the views of the data subjects required prior to go-live? | No, but patients will be contacted and asked if they wish to participate. |
| In which country will the data be held? | UK |
| Will any personal data be transferred to another organisation? | There will be an initial sharing of patient details and this will be completed using NHS mail.  Access to SystmOne healthcare records only. Personal Data will not be transferred or held in any other form by the service provider. |
| Will any personal data be transferred outside the UK? \* | No |
| Will any NHS patient personal data be transferred to another organisation for reasons other than the patient’s individual care? \*\* | No |

*\* It is a contractual requirement that personal data processed for the NHS is not transferred outside the UK.*

*\*\* If answered yes, this may fall within the scope of the NHS national data opt-out.*

* 1. The processing operation for the project is documented below:

|  |
| --- |
| **Data Processing Operation** |
| As a result of the COVID19 pandemic, cohorts of vulnerable patients across BSW may have missed their annual health check. Due to the ongoing pressures on GP Practices as they respond to COVID19, First Option Healthcare will book appointments and conduct the health checks.  The health checks will include a lateral flow test if they present and COVID19 is suspected. Once the team are established, COVID19 vaccinations may also be provided.  **Outline processing operation**   1. To send briefing email or letter [to those who have provided consent to participate via the health care record] regarding the new annual health check (AHC) offer [letter to be sent to all on the SMI & LD registers] letters to be sent by either GP surgery or FOHC [GP surgery to determine favoured approach].   To send the letter, SystmOne or EMIS access required to obtain addresses for those on the SMI & LD registers.   1. First Option Healthcare (registered nurses and health care assistants) to contact those [again those consenting] via phone to book their appointment for the AHC.   To complete the phone calls to offer the opportunity to book and appointment – access to SystmOne or EMIS will be required to obtain phone numbers and record the outcome of the offer ie. Appointment booked or not.   1. For those choosing to have an ANC, First Option Healthcare (registered nurses and health care assistants) will need to review the patients’ health records (System one and EMIS) in advance of their appointment to ensure they understand their health status baseline and can subsequently record the outcome of their assessment.   The PCN admin team will be asked to provide admin resource to help identify the patients via the patient records and send the emails. Patients that do not have an email will require a letter.  In the event the PCN do not have the resource to process and send the letters, First Option Healthcare will identify and send out the initial communications (Email or letters) to patients.  First Option Healthcare are CQC registered and submit an annual NHS Digital Data Security & Protection toolkit submission. Their nurses will use NHS Smartcards to access clinical systems and have access to NHS.net secure email.  Initially, during the pilot, individual GP practices will need to provide the First Option Healthcare staff with access to their local patient management system (SystmOne).  After the pilot, access to the CCG POD instance of SystmOne will be provided for First Option Healthcare to allow them to review records in advance of health checks and write up notes after health checks.  First Option Healthcare could potentially use DocMan as a method to update patient records for those patients registered at EMIS practices.  First Option Healthcare are responsible for providing their staff with the necessary laptops, smartcard readers, secure remote connection and software (TPP SystmOne) in order to deliver the service.  First Option Healthcare will work with Bath Mind and Swindon & Gloucestershire Mind to increase update of the health checks. This will include FOHC sharing booking lists with Bath Mind and Swindon & Gloucestershire Mind as they are often familiar with the patients and can advise or better connect with them to improve uptake and opt-in.  A specific data sharing agreement between the pilot practices and First Option Healthcare is not required for this service in response to the COVID19 pandemic as the data sharing aspect is covered (for COVID19 purposes) by the Notice under regulation 3 (4) of the Health Service Control of Patient Information (COPI) Regulations 2002, issued 20 March 2020 and extended until 30 September 2021.  The BSW CCG is commissioning First Option Healthcare to provide the health check service via an NHS standard contract (short form) which includes data protection clauses and a data protection protocol. This will cover all instances and requirements of First Option Healthcare and Bath Mind and Swindon & Gloucestershire Mind processing personal data including accessing the patient records via SystmOne.  Any potential personal data breaches or breaches of patient confidentiality will be reported to the Patients registered GP Practice in the first instance. |

**Further details on how the data processing will comply with the GDPR Principles relating to processing of personal data are captured in section 9**

# Assessment of Necessity and Proportionality

* 1. Answer the following questions to confirm that the necessity and proportionality of the processing has been assessed in relation to the purpose of the data processing:

|  |  |
| --- | --- |
| **Question** | **Yes or No** |
| Is the processing of the identified personal data necessary for the project? | yes |
| Is the processing of the identified personal data in proportion to the purpose of the project? | yes |

# Assessment of Risks to Data Subjects

* 1. The details of any risks related to individuals and compliance as a result of this project are detailed below:

|  |  |  |
| --- | --- | --- |
| **Issue** | **Risk to Individuals** | **Compliance Risk** |
| External organisations accessing patient medical records. | Patient personal data will be accessible by additional individuals and therefore potential higher risk of data quality/breaches. | Potential personal data breach. |
| Clinical system not available | Potential loss of personal data due to clinical system not being available | Potential personal data breach |

# Measures to Address Risks to Data Subjects

* 1. The actions taken to reduce the risk of any data protection issues identified in section 6.1 are detailed below:

|  |  |  |
| --- | --- | --- |
| **Risk to Individuals** | **Solution** | **Result** |
| Patient personal data will be accessible by additional individuals and therefore potential higher risk of data quality/breaches. | First Option Healthcare clinicians are registered nurses and existing processes and policies in place to control the use of patient personal data. | Risk mitigated to an acceptable level. |
| Potential loss of personal data due to clinical system not being available | BC Plan – standard template used to capture information and sent to registered GP practice via NHS mail for upload to patient record. | Risk mitigated to an acceptable level |

# Prior Consultation

* 1. It is a requirement of the GDPR to consult with the ICO **prior to processing** where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the practice to mitigate the identified risk or risks.
  2. Answer the following questions to identify if there is a requirement to consult the ICO:

|  |  |
| --- | --- |
| **Question** | **Yes or No** |
| Do any risks remain unmitigated? | no |
| Does an unacceptable level of risk remain? | no |
| Is it likely that data subjects may encounter significant, or even irreversible consequences, which they may not overcome? | no |

*If any of the above questions have been answered as “Yes”, than it is a mandatory requirement to consult with the ICO before commencing the project.*

# Association with the GDPR principles

The following section demonstrates how the project will be implemented to ensure compliance with the GDPR:

* 1. Principle A – Lawfulness, Fairness and Transparency

|  |  |
| --- | --- |
| **Compliance Question** | **Summary** |
| Does the project have an identified purpose? | Yes, to allow First Option Healthcare to book and complete health checks for cohorts of vulnerable patients. |
| What is the lawful basis for processing the personal information? | Article 6, 1 (e) Public task  Article 9, 2 (h) Health or social care |
| How will individuals be informed about the use of their personal and/or special categories of personal data? | Privacy notice  Consider vulnerable patients – is Privacy Notice adequately worded and accessible?  Patients will be contacted and asked if they wish to participate and will be advised the health check will be provided by First Options Healthcare. |
| Do you need to create or amend a privacy notice? | The practice will need to review their privacy notice in line with the latest template to ensure it includes sharing personal data with other healthcare providers.  The CCG will review privacy notice in light of CCG providing the service provider access to the POD TPP instance. |
| If consent will be used as the lawful basis, how will consent to process personal data be captured and what will you do if it is withheld or withdrawn? | Consent not relied upon as a lawful basis to process personal data. |

* 1. Principle B – Purpose Limitation

|  |  |
| --- | --- |
| **Compliance Question** | **Summary** |
| Does the project plan cover all of the purposes for processing personal and/or special categories of personal data? | Yes, the scope of the project is limited to facilitate the booking and delivery of health check appointments. |
| Has the project plan identified potential new purposes as the scope of the project expands? | No, any additional purposes identified will result in a review of the DPIA. |

* 1. Principle C – Data Minimisation

|  |  |
| --- | --- |
| **Compliance Question** | **Summary** |
| Is the quality of the information good enough for the purposes it is used? | Yes, information will be read and entered directly into SystmOne. |
| Which personal and/or special categories of personal data could the project not use, without compromising the needs of the project? | Name  Address  Phone number  Date of birth  NHS Number  SMI & LD code  For those booking an AHC – review of electronic primary care health record for the purposes of providing a baseline understanding of wellbeing. |

* 1. Principle D - Accuracy

|  |  |
| --- | --- |
| **Compliance Question** | **Summary** |
| If the project involves the procurement of new software, does it allow for data to be amended when necessary? | n/a |
| What measures will be in place to ensure that personal and/or special categories of personal data obtained from individuals or other organisations is accurate? | ‘new’ information obtained will relate to outcomes of health care check only. This will be validated by the practitioner completing the check, and recorded on the patients electronic health care record, with any follow up actions flagged for the attention of the patients GP. |

* 1. Principle E – Storage Limitation

|  |  |
| --- | --- |
| **Compliance Question** | **Summary** |
| What retention periods are suitable for the personal and/or special categories of personal data that will be processed? | 10 years post patient death, as specified in the Records Management Code of Practice for Health and Social Care 2016 (2020 version still in draft and not yet approved for use). |
| If the project involves the procurement of new software, does it allow for data to be deleted? | n/a |

* 1. Principle F – Integrity and Confidentiality (Security)

|  |  |
| --- | --- |
| **Compliance Question** | **Summary** |
| Do any new systems provide protection against the risks to individuals identified in this DPIA? | n/a |
| What are the training and documentation requirements to ensure that staff know how to operate the new system securely | Staff will be trained to record the outcome of health care checks on SystmOne/EMIS. |
| If there is a requirement to transfer personal and/or special categories of personal data, what measures will be put in place to ensure the protection of the data? | Additional information will be entered directly into the patients’ clinical record on SystmOne.  Any BC or ad-hoc communications including patient personal data will be completed using the secure NHS Digital NHS mail service. |

# DPO Recommendations

|  |  |
| --- | --- |
| **No.** | **Recommendation** |
| 1. | The practice will need to review their privacy notice in line with the latest template shared by the DPO to ensure it includes sharing personal data with other healthcare providers. |
| 2. | The CCG may need to review their privacy notice in relation to FOHC having access to the CCG POD SystmOne instance. |