## You Matter DPIA

# Step 1: Identify the need for a DPIA

|  |
| --- |
| Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA. |
| Staff wellbeing and associated mental health has become a priority for NHS England as a result of the Covid19 pandemic, leading to funding of new services.  You Matter (YM) is being established on behalf of the ICS which covers Buckinghamshire, Oxfordshire and Berkshire. YM provides a service to the whole range of staff groups working in the NHS, Primary and Social Care in Buckinghamshire and Oxfordshire although staff from West Berkshire may use it. West Berkshire are providing a second hub for use by staff living or working in that area. (YM) is a Mental Health and Wellbeing Hub for staff aged 16 and over. It aims to provide rapid access, assessment and triage to those staff who choose to consent to share PID. Those hard to reach staff who do not consent but are concerned about their Mental Health, will be offered a signposting and information sharing service though the use of pseudonyms. Although initiated during the Covid 19 pandemic, it is intended that the service will continue after this initial health crisis as mental health problems will continue to emerge for many years afterwards. Following screening staff who need it will be referred or signposted to appropriate mental health services for treatment as this will not be available within the Hub which may include EAPs. The YM hub will be hosted in the IAPT TalkingSpace Plus service.  There is a need for a DPIA as YM will be processing personal data of staff who may or may not choose to become patients. We need to ensure that the highest levels of data security and confidentiality are afforded to them in order to enable staff to use YM with ease.  YM transmits and transfers data to the Trust and any other party with the consent of the staff member or when their risk to themselves or others necessitates this.  The Trust determines what personal data is obtained, stored, and processed by YM. |

# Step 2: Describe the processing

|  |
| --- |
| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved? |
| Staff members will contact YM by phone or email. The only information they provide at this stage is a name and preferred method of contact (phone or email). PID is only collected if the staff member consents to share their details, although this is not a requirement for receiving a service. They are booked into a screening call where clinical information is obtained. All PID and clinical information is stored on a unique pathway in PCMIS, the electronic health recording system used in both IAPT services in OHFT. YM PCMIS account will be completely separate and held on a separate server to both OHFT IAPT PCMIS accounts.  You Matter staff have access to the electronic health record on PC-MIS through a secure logon. Regular audit will be undertaken by the Clinical Service Lead or her deputy to ensure that access is undertaken strictly for clinically relevant purposes only.  The Trust is a data controller and YM is the data processor. The Trust determines what personal data is processed and stored on PCMIS. Although data is not routinely shared with anyone else YM will, if judged necessary following as complete a risk assessment as possible, and after making all reasonable efforts to seek consent from the person accessing the service:  a) Send personal information to GP, Adult Mental Health Services, emergency services.  b) Alert employers that the staff member is at risk to themselves or others.  c) Alert registering professional organisations e.g. GMC, HCPC etc. |

|  |
| --- |
| **Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? |
| YM collects demographic and clinical PID from staff members using the service which it processes and stores in the electronic health record system called PCMIS (YM Pathway). PCMIS complies with all NHS data standards and information governance.  YM is being established on behalf of the ICS which covers Buckinghamshire, Oxfordshire and West Berkshire. YM in particular provides a service to people working in the NHS, Primary and Social Care in Buckinghamshire and Oxfordshire although staff from other areas may use it. It is estimated 50,000 staff are employed in health and social care in this area and there is a high turnover in employment. Staff from West Berkshire who choose to use YM because they are concerned about using a mental health service run by their employer will also be accepted. Data collected includes clinical and personal information which YM or staff members decide is relevant to their current mental health needs. Access to this data is by secure log on and there is an audit trail of staff accessing these health records. The data will be stored for a minimum of 8 years.  The data will be collected at the following points:   1. Phone contact 2. Screening call 3. Additional calls as required to complete the screening and to develop a treatment plan   The data will be used at the following points   1. To create an electronic record 2. To contact the person to arrange a screening 3. To develop a treatment plan 4. To report on the functioning of YM to NHS England using anonymized data. Under no circumstances will any PID be shared with NHS England 5. To share information with clinical colleagues about the service using anonymized data either to support more self-referrals to the service or to enable colleagues in other places to learn about the development of YM as a Staff Mental Health and Wellbeing Hub. |

|  |
| --- |
| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? |
| 1.Staff members who contact YM may choose not to give their PID and to obtain signposting only from us. Data from this type of contact will be anonymous and stored in a file on Teams - date and time of call, broad nature of enquiry and any information given, and will be used in the development of the service.  2. Following a comprehensive communication of the extent of data processing including terms and conditions of information handling by YM, some staff members will consent to provide PID via a phone call or email.    3. YM will not routinely collect information regarding children.  4. The process of gaining consent will give the staff member full understanding of the extent of data processing so they will expect YM to use their data in this way. An electronic or hard copy of a staff member / service users guide to information processing at YM- Terms and Conditions will be available to them.    5. There are no concerns about the PCMIS pathway electronic health records system which is a tried and tested platform. There is no novel addition to this pathway.  6. The most significant concerns are ease of access for staff to mental health services and related to this, the right of all health and social care staff to be treated in a service which respects their confidentiality at every step of the way which at one extreme would mean that YM staff could actually ask to access the service themselves.  7. Utilising existing technology (PCMIS) and no public concerns. |

|  |
| --- |
| **Describe the purposes of the processing:** what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly? |
| Data is processed to report to NHS England to demonstrate the performance of YM. An example of this is given here:  *A8. Of the staff assessed (A3) how many were clinical staff (excluding medical or nursing/midwifery staff) e.g. healthcare assistants, therapists etc? Note not all staff may wish to share personal information*  No more detailed information is shared with MNHS England than the example given above.  Individuals who contact YM with concerns about their mental health are advised, and if necessary signposted or referred to appropriate services with their consent or in the case of a clinical emergency without. YM cannot run a clinical service without comprehensive confidential clinical recording and reporting. |

# Step 3: Consultation process

|  |
| --- |
| **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts? |
| We have consulted with (those at 2,3,4 attend a regular YM steering group)   1. OH Head of Information Governance- MU 2. OH Head of wellbeing and Stress RO’N 3. OH Associate Director of Psychological Therapies BT 4. Jo Ryder and John Pimm – Clinical and Professional Leads PTP and Head of IAPT (Oxon & Bucks) |

# Step 4: Assess necessity and proportionality

|  |
| --- |
| **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? |
| YM will have its own PCMIS account independent of the OHFT IAPT services. An audit trail will be available to ensure that these named individuals only access information that is necessary to their work.  The YM clinical lead (DC) will report to the service steering group and be guided by them on any matters relating to function creep.  As this is a new service, information reviews will be undertaken to ensure data quality and date minimization.  Other services will only be given information with consent from staff contacting YM except in clinical emergencies – see above. An electronic or hard copy of the service guide to information processing at YM - Terms and Conditions will be available to them. |

# Step 5: Identify and assess risks

|  |  |  |  |
| --- | --- | --- | --- |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risksas necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
| Risk of data loss  Risk of data compromise  Risk of system unavailability  Risk of system misuse  Fair and lawful processing  Staff member trying to access YM as patient is recognized as colleague by clinician in YM  Rag Rating: Risk Low  *Acceptable risk. Identified threats must be monitored to understand if the risk level needs to be increased.* | Remote, possible or probable  Remote  Remote  Remote  possible | Minimal, significant or severe  Significant  Significant  Significant  significant | Low, medium or high  Low  Low  Low  low |

# Step 6: Identify measures to reduce risk

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5** | | | | |
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
|  |  | Eliminated reduced accepted | Low medium high | Yes/no |

# Step 7: Sign off and record outcomes

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/date** | **Notes** |
| Measures approved by: | No actions required | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: | No high risk processing | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: | No processing, acceptable privacy Notice provided to users | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice:  None. | | |
| DPO advice accepted or overruled by: |  | If overruled, you must explain your reasons |
| Comments: | | |
| Consultation responses reviewed by: |  | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: | | |
| This DPIA will kept under review by: | Passed – 30/03/2021 | The DPO should also review ongoing compliance with DPIA |