## **Data Privacy Impact Assessment (DPIA)**

# Submitting controller details

***UK Biobank Exemplar DPIA: prepared by UK Biobank as a suggested format to help GP Practices readily incorporate the relevant information about UK Biobank into a DPIA form (although it is for each GP Practice to conduct its own DPIA assessment).***

|  |  |
| --- | --- |
| Name of controller | The Scott Practice |
| Subject/title of DPIA | **UK Biobank Extract for Consented Participants** |
| Name of controller contact /DPO  (delete as appropriate) | The Scott Practice  DPO Dr Dean Eggitt |

# 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. |
| * The practice has been approached by UK Biobank, a national research study, requesting a regular pseudonymised extract of health records for its participants that are patients of this practice. * It may be the case that this represents a change in scope to current processing within the practice and, as such, a Data Privacy Impact Assessment has been undertaken. * The data to be processed are special category as they relate to the health of individual patients. * There is a clear legal basis for this extraction and processing as all UK Biobank participants have provided their explicit consent for UK Biobank to access all of their medical and health-related records. UK Biobank is also entitled to rely on the ‘legitimate interests’ basis in the GDPR. These bases for extraction and processing are clearly set out in UK Biobank’s communication to their participants [https://www.ukbiobank.ac.uk/gdpr](https://www.ukbiobank.ac.uk/gdpr/). * The proposed data extract will be undertaken by the GP system software supplier (EMIS ) using a tested extraction mechanism and will require little (if any) interaction by the GP practice (other than accepting a data-sharing request). * The GP practice will have the ability to audit the extraction process to determine those patients for whom data have been extracted and made available, in a secure manner, to UK Biobank. * The proposed processing utilises existing technology components and is regarded as a low risk to individual patients (due to the secure manner of the data extract approach and the subsequent de-identification of data before onward use by researchers). To date, there is no known instance of a UK Biobank participant being re-identified by the provision of data to researchers. * Further information regarding the extraction process can be found online at <http://www.ukbiobank.ac.uk/general-practice>. |

# 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? |
| * There is no change to the information that we collect, use, store or delete within the practice. * The source data for this extract is the GP practice healthcare record (albeit it will be taken from operational secondary repositories to avoid placing undue demand on primary systems). * We will be given the ability to identify which of our patients are participants of UK Biobank (and will be able to denote their participant status by adding relevant coding to their records). * The proposed processing relates solely to the sharing of healthcare data (in coded form only) for UK Biobank participants who have all provided their explicit consent. |

|  |
| --- |
| **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? |
| * The scope of the extract relates to patients within the GP practice who are consented UK Biobank participants. The number of individuals in scope will vary over time as UK Biobank participants leave or join as patients of the GP practice. * UK Biobank estimates that a GP practice might typically have approximately 10 participants per practice, although a very limited number of practices may have over 1,000 participants; in any event, this will not represent large-scale processing at a GP practice level. * The data to be extracted are coded healthcare-related events (e.g. consultations, investigations and prescriptions). Given the healthcare nature, they represent special category data. * The data that will be extracted will be pseudonymised. This means that UK Biobank will have the ability to link the pseudonymised health record data to the corresponding participant data that it retains within its resource. However, UK Biobank only releases de-identified data to researchers. * Repeated data extracts will be conducted at intervals (intended to be approximately annually) for all consented participants who are registered at the GP practice. |

|  |
| --- |
| **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)? |
| * The data relate to patients of the practice who are also UK Biobank consented participants. * UK Biobank participants maintain full control, and can withdraw from UK Biobank unilaterally for any reason at any time by simply contacting UK Biobank directly. * UK Biobank maintains an audited withdrawal process and will ensure that participants who have elected to withdraw are not included in any future extract. * Participants who are patients at this practice would expect their health record data to be used in this way as they have provided explicit consent (witness the consent form) and this was based on clear guidance provided in participant literature (which in turn had been extensively reviewed by external ethics boards) <https://www.ukbiobank.ac.uk/general-practice>. * UK Biobank already links to secondary health record data for its participants. It also maintains regular contact with its participants through newsletters and updates. UK Biobank contacted all of its participants last year – see the link on the UK Biobank website – to confirm how it processes their data under GDPR <https://www.ukbiobank.ac.uk/gdpr>. * UK Biobank participants were aged between 40 and 69 at the time of recruitment in 2006-2010 and, as such, the processing does not involve data from children. * The process uses existing technology to support data extracts; matching algorithms have been used in prior studies, and no novel technology is being proposed. * The Information Commissioner has confirmed that UK Biobank’s approach to obtaining these data for consented UK Biobank participants complies with the General Data Protection Regulation. The Joint IT Committee of the RCGP/BMA has endorsed UK Biobank’s process for this data extraction. * There should be no issues of public concern. |

|  |
| --- |
| **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? |
| * As a practice, we recognise the consent that UK Biobank participants have provided to UK Biobank, which includes the ability to link to their healthcare records. * UK Biobank is one of the leading resources in the world for the conduct of health-related research. It is a leader in providing data for a large number of research projects. To date, its custodianship of the UK Biobank resource (and the data within it) has been entirely robust and secure, such that its processes and protocols are used by other resources around the world. * For UK Biobank, access to these primary care records will substantially enhance the research capabilities of the UK Biobank resource. For example, it will enable certain diseases (such as diabetes and dementia, where the main patient record is in the primary care sources) to be studied in greater depth. * This increase in UK Biobank’s research capability has been endorsed by, amongst others, the Secretary of State for Health, the Chief Medical Officer for England, and the Head of NHS Digital. * Such enrichment will enhance the value of the UK Biobank resource and provide benefit to the research community to improve the prevention, diagnosis and treatment of a wide range of serious and life-threatening illnesses. |

# 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? |
| * The GP practice will add UK Biobank to the list of approved research organisations listed in the practice’s data privacy and processing notice (as published in our practice surgery). * UK Biobank has made available their signed electronic consent forms via an online service. The practice does not need to engage with individual patients to confirm their consent since a participant could not take part in the UK Biobank study without providing their explicit consent and there would be no impact on the participant as a result of providing these data to UK Biobank. * The proposed data extract has been reviewed by the ICO, NHS Digital, the RCGP, and the Joint RCGP/BMA IT Committee, all of whom support UK Biobank’s approach. * UK Biobank has engaged with EMIS as the data processor to ensure that the data are extracted in secure and robust manner. * This DPIA has been reviewed and approved by our DPO. |

# 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? |
| * The lawful bases for this processing are the explicit consent provided by UK Biobank participants and UK Biobank’s legitimate interests. * UK Biobank has recently written to all of its participants setting out its own legal bases for the processing of data: <https://www.ukbiobank.ac.uk/gdpr/>. * This data extract will achieve the purpose of respecting the expressed wishes of UK Biobank participants for making their data available to UK Biobank for this purpose. * UK Biobank is seeking access to coded information only within the primary care record. * UK Biobank is able to ensure that only data relating to UK Biobank participants is extracted by providing their identifiers (NHS number, date of birth and gender) in an encrypted format via secure transfer for the purpose of precisely matching to relevant records. Only the matched participant records from a practice will be extracted by the practice’s system supplier. * Extracted data are returned to UK Biobank in a similarly encrypted format and via secure transfer. Information released by UK Biobank to approved researchers is provided in a de-identified format such that it is not possible for researchers to re-identify any participant. * The practice will update its privacy notice and processing register, and will include UK Biobank as a named entity to which it provides data for consented participants. * The practice will have the ability to audit those patients for whom data have been extracted. |

# 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**  Remote, possible or probable | **Severity of harm**  Minimal, significant or severe | **Overall risk**  Low, medium or high |
| The risks identified below are included as examples that GP practices may wish to consider as part of its assessment.   * There is a risk that mismatching means patients within the practice may be incorrectly identified as UK Biobank participants. [*Matching process has been tested and is based on combination of NHS ID / Gender / Date of Birth to ensure accurate matching*] * There is a risk that personal / identifying information may be extracted. [*Only coded data are being extracted and specific codes that may be potentially identifying have been excluded*] * There is a risk that a data breach may occur in the transfer of data between the practice system and UK Biobank. [*Data extraction is being undertaken in a secure, automated environment, and will be appropriately encrypted and securely transferred direct to UK Biobank*] * There is a risk that the practice is not compliant with data protection regulation (including the GDPR). [*There is a clear legal basis for consent, the extraction process has been reviewed and is endorsed by several bodies including the ICO, NHS Digital and the RCGP*] * There is a risk that data are extracted for participants for whom consent is not in place. [*Only participants who provided explicit consent were able to take part in the UK Biobank study. UK Biobank maintains an auditable withdrawal process. No withdrawn participants will be included within the extract*] | Remote  Remote  Remote  Remote  Remote | Minimal  Minimal  Minimal  Minimal  Minimal | Low  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** | |
| * There is a risk that mismatching means patients within the practice may be incorrectly identified as UK Biobank participants. [*Matching process has been tested and is based on combination of NHS ID / Gender / Date of Birth to ensure accurate matching*] * There is a risk that personal / identifying information may be extracted. [*Only coded data are being extracted and specific codes that may be potentially identifying have been excluded*] * There is a risk that a data breach may occur in the transfer of data between the practice system and UK Biobank. [*Data extraction is being undertaken in a secure, automated environment, and will be appropriately encrypted and securely transferred direct to UK Biobank*] * There is a risk that the practice is not compliant with data protection regulation (including the GDPR). [*There is a clear legal basis for consent, the extraction process has been reviewed and is endorsed by several bodies including the ICO, NHS Digital and the RCGP*] * There is a risk that data are extracted for participants for whom consent is not in place. [*Only participants who provided explicit consent were able to take part in the UK Biobank study. UK Biobank maintains an auditable withdrawal process. No withdrawn participants will be included within the extract*] | Patients are matched against the Spine when registered so mismatching is a minimal risk  No personal/identifying information should be extracted as specific third party codes have been excluded from the extraction process  This is a minimal risk as extraction systems are encrypted and secure  The practice has confirmed with patients who are registered with Biobank that they receive regular letters from Biobank giving them regular reminders of their registration and the information Biobank would be extracting.   * The practice has written to all patients identified as having consented to Biobank, advising them of the extraction request and giving them the opportunity to withdraw consent from Biobank if they choose to do so | Remote  Remote  Remote  Remote  Remote | | Minimal  Minimal  Minimal  Minimal  Minimal | | | yes  yes  yes  yes  yes | |
|  | | |  | |  |  | |

# Step 7: Sign off and record outcomes

|  |  |
| --- | --- |
| DPO advice: Approve processing?  In essence, the risk mitigation is detailed as follows:        The practice has been approached by UK Biobank, a national research study, requesting a regular pseudonymised extract of health records for its participants that are patients of this practice.        It may be the case that this represents a change in scope to current processing within the practice and, as such, a Data Privacy Impact Assessment has been undertaken.        The data to be processed are special category as they relate to the health of individual patients.        There is a clear legal basis for this extraction and processing as all UK Biobank participants have provided their explicit consent for UK Biobank to access all of their medical and health-related records.  UK Biobank is also entitled to rely on the ‘legitimate interests’ basis in the GDPR.  These bases for extraction and processing are clearly set out in UK Biobank’s communication to their participants [https://www.ukbiobank.ac.uk/gdpr](https://www.ukbiobank.ac.uk/gdpr/).        The proposed data extract will be undertaken by the GP system software supplier (EMIS ) using a tested extraction mechanism and will require little (if any) interaction by the GP practice (other than accepting a data-sharing request).        The GP practice will have the ability to audit the extraction process to determine those patients for whom data have been extracted and made available, in a secure manner, to UK Biobank.        The proposed processing utilises existing technology components and is regarded as a low risk to individual patients (due to the secure manner of the data extract approach and the subsequent de-identification of data before onward use by researchers).  To date, there is no known instance of a UK Biobank participant being re-identified by the provision of data to researchers.    Roy  HARRIS, Helen (NHS DONCASTER CCG)  Wed 28/08/2019 12:08  Inbox  **To:**  FELLS, Rose (NHS DONCASTER CCG);  **Cc:**  UNDERWOOD, Roy (DONCASTER AND BASSETLAW TEACHING HOSPITALS NHS FOUNDATION TRUST);  Hi Rose    DPIA approved by myself and the DPO – Roy Underwood with the risk mitigation detailed above by Roy.    Kind regards    **Helen Harris Head of Corporate Governance** Direct Dial 01302 566300 Ext 1216  Email: [helen.harris31@nhs.net](mailto:helen.harris31@nhs.net)  DPO Signature: | |
| DPO advice accepted or overruled, if overruled provide reasons: |  |
| Reasons: | |
| This processing and this DPIA will be kept under review, next review date: |  |