A black background with a logo

Description automatically generated

**Data Protection Impact Assessment**

**DPIA\_183 v3 Approved**

**Version control**

|  |  |  |
| --- | --- | --- |
| **Version** | **Notes to summarise changes** | **Approved date** |
| **V2** |  | **5 July 2023** |
| **V3** | **The changes would allow us to store YNIC data on University servers, not just YNIC servers.** | **20th October 2023** |

**Primary contacts**

|  |  |
| --- | --- |
| Durham Burt  **Data Protection Officer**  [dataprotection@york.ac.uk](mailto:dataprotection@york.ac.uk) | York NeuroImaging Centre (YNiC) Research  Fiona McNab  Chair of Ethics YNiC Research Ethics Committee  Andre Gouws  Operations Manager |

**Step 1: Identify the need for a DPIA**

|  |
| --- |
| **Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer to or link to other documents, such as a project proposal or ethics application form. Summarise why you identified the need for a DPIA.** |
| Background:  The York Neuroimaging Centre (hereinafter YNiC) is a research facility of the Department of Psychology. Research carried out at the centre falls within the research governance framework of the Department of Psychology. However, some of the specialist techniques used at the centre have associated data acquisition, handling and storage requirements that would not apply to the majority of research projects in the Department of Psychology. The purpose of this DPIA requirement is twofold: (1) to define the data risks and mitigations related specifically to research activity, processes, policies and procedures at YNiC and (2) to provide a “blanket” DPIA for research projects carried out at YNiC that conform to and comply with standard procedures described in this document.  In order to understand the potential risks of data mishandling, it is important to consider the stages of data acquisition of a YNiC project, the nature of the data being acquired at those different stages and the responsibilities and procedures defined at each stage. The data acquisition process can be summarised as in the matrix below:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Stage of research project | What is the process and purpose of acquiring data? | What is the nature of the data? | Who can gain access to data? | Who is responsible for data storage / security? | | 1  Participant recruitment and pre-acceptance screening (i.e. screening before any data is stored on University of York systems) | Questionnaires completed verbally by phone or using online forms to ascertain suitability of participants to take part in the project | Will include:  \* Personal information  \* some health information / information regarded as medically sensitive  May include:  \* lifestyle choice information regarded sensitive | All named investigators on the project | Primary investigator on project | | 2  Registration on University of York systems (usually days / weeks in advance of scans) | \* Participant consents to policies and procedures and is notified that consent can be withdrawn at any time   \* Participant information is added to the secure database and a unique pseudo anonymised ID is generated  Uses referenced docs:   \* YNIC General Consent Form | Will include:  \* Personal information  \* Contact information  for the participant’s GP  \* some health information / information regarded as medically sensitive | YNiC staff  All named investigators on the project that request access | YNiC staff  Primary investigator on project once access requested | | 3  Study specific information and assessments (may be pre and/or post scan data acquisition) | Questionnaires to gather study specific consent  Personal, study-relevant task performance information  Uses referenced docs:   \* Study Specific Consent Form   \* Study Specific Participant Information Form | Will include:  \* Personal information  May include:  \* some health information / information  regarded as medically sensitive  \* lifestyle choice information regarded sensitive  \* study-specific task performance data | All named investigators on the project | Primary investigator on project | | 4  On the day of the scan - Safety screening forms | Questionnaires to ensure   \* Participant does not have any personal physical traits or medical history which means they are at risk at the time of the scan   \* participant consents to take part at the time of the scan  Uses referenced docs:   \* MRI / MEG / TMS safety screening forms | Will include:  \* Personal information  \* some health information / information regarded as medically sensitive  May include:  \* lifestyle choice information regarded sensitive | YNiC staff and approved University of York IT staff  Named investigators on the project present at the time of procedure | YNiC staff and approved University of York IT staff | | 5  Storage of and access to acquired scan data | Data acquired on the scanner is pseudo-anonymised and stored on University of York  servers for access by authorised users. The servers are physically secured and only accessible by members of YNiC technical staff and approved University of York IT staff. Data is secured by authentication with admin access limited to the YNiC Staff and approved University of York IT staff. YNiC users access to pseudo-anonymised data is available after agreeing to the YNiC Data Protection policy.  Uses referenced docs:   \* YNIC Data Protection Policy and YNiC Appropriate  Data Usage Declaration. | Will **not** include:  \* Immediately identifiable personal  information (name, DOB, Address, medical, info, etc)  May include:   \*  special category personal information (akin to “biometric data”) | YNiC staff and approved University of York IT staff  Named investigators on the project present at the time of scan | YNiC staff and approved University of York IT staff  Named investigators on the project if they request to make a physical copy of such data not stored on YNiC systems. |   The participant recruitment process for YNiC research involves asking the potential participant a number of screening questions. Data from some of these questions may be classed as “special category personal data” as they relate to health.  Such questions may be asked (i.e. data may be collected) at stages 1 and 3 in order to determine whether that person belongs to a population of interest (eg. whether they are neurologically healthy etc.)  Further special category personal data questions asked at stages 1, 2 and 4 allow us to determine whether it is safe for that person to participate (eg. exposure to a magnetic field poses a risk for specific individuals who have medical devices implanted in their bodies).  Furthermore, Magnetic Resonance (MR) data, even when stored in a pseudorandomised manner as in stage 5 above, may be considered “**special category personal data**”. Some MRI data can be reconstructed in such a way that they could be considered to reveal “biometric information”. For example, it is not unusual for MRI / MEG / TMS data processing to require that the participant's head shape (and thus face) be reconstructed in 3D from an MRI scan. Although such reconstructions are inherently noisy, they do offer a potential mechanism for identification of a subject from their pseudo-anonymised MRI data. Arguments have also been made that the sulcal and gyral folding patterns and configuration of the brain are unique to each person and thus represent a potential “brain fingerprint”. Crucially, and worth noting, if you were trying to identify an individual from pseudo-anonymised MRI data, you would need to have access to a non-anonymised reference dataset specifically linked to that individual in order to make a comparison. That is to say you would explicitly be trying to unmask the identity of a participant from data you have acquired from a known individual. This would be contrary to all data protection policies already in place at YNiC. It could also represent a breach of section 171 of the Data Protection Act 2018:  *It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.*  Lastly, any person giving consent to participate in a research study at YNiC will, at stage 2 above, need to provide consent for us to contact their GP in the case that the procedures carried out at the centre reveal a medical anomaly that may require further investigation or medical information. YNiC holds this special category of personal data in a secure database. Database software has multiple levels of access control and it stored on the secure servers. Within YNIC, only three users have full access, the IT manager and the two directors. When stored on University of York servers, only approved University of York IT staff will have access. Regular patching is performed on the database and supporting software and security patches are applied as soon as available. Backups of the data are taken nightly, encrypted and stored in a fire proof safe. Only YNiC staff have access to the safe.  To summarise, potentially sensitive data will be acquired and processed as follows:   * Stage 1 - Initial screening questions asked by an individual researcher. These vary from study to study depending on the methods used and the population of interest. Researchers will capture this information using a Google form (managed by the individual research groups), either filled in by the participant or by the researcher on behalf of the participant. Researchers will ask participants to read the YNiC safety forms relevant to the modality of scanning to be carried out (i.e. MRI, MEG or TMS, or any combination of them) and will ask participants to confirm that there are no contraindications on those forms that mean that they cannot safely take part in the study. These data are held by the investigators. * Stage 2  - A general consent form issued by and held at YNiC is completed by the participant confirming their consent to participate, and that YNiC will contact their GP in the case that an anomaly is found. Participants are added to a secure database and a pseudo-anonymised ID is generated for them. Data are held by The University of York. * Stage 3 - The participant completes the study specific consent form after reading the study specific information sheet. The participant completes behavioural / additional experiments that complement the measures made at YNiC. Data are held by the investigators. * Stage 4 -  The participant attends YNiC to have the procedures (“scans”) carried out  - any of the 3 relevant safety screening forms (MRI, MEG , TMS) are completed. Data are held by YNiC. * Stage 5 - Data from the scanners are transferred to University of York servers for access by investigators. These data are stored in a pseudo-anonymised format. These data can be accessed by investigators who agree to abide by all YNiC data protection policies and procedures. These policies include a declaration signed by each investigator which  confirms that investigators will not use pseudo-anonymised data to try to determine the identity of the person from whom it was obtained. Data are held on University of York servers, but investigators may ask for permission to hold off site copies at which point investigators become responsible for the data and should complete their own DPIA if their study is not covered by the data sharing procedures described below.   In addition to the procedures described above, this modified DPIA covers public sharing of YNiC data, in particular MRI (brain) data. Universities, funders, and journals increasingly often require free sharing of research data, to make the most of these data, which are often expensive financially and in terms of the participants’ time. As described above, MRI data can be classified as personal (potentially special category) data. To allow for sharing of these data, participants will be informed of data sharing procedures in the revised Study Specific Participant Information Form (Version 9) and are asked to give consent in the Study Specific Consent Form (Version 9). Participants can only take part in a study if they consent to data sharing, as outlined in the Participant Information Form.  The Participant Information Form describes several ways in which data can be shared, including sharing on public platforms. Researchers can only use these templates if they follow the default procedure of defacing the MRI data to minimise risk of participant identification. The resulting risk of identification based on defaced MRI data is very low. Without additional non-anonymised data, identifying a participant based on MRI data (including self-identification) is extremely difficult.  Furthermore, prior to sharing these data publicly, researchers will submit a request for data file renaming to YNiC staff, who will check they have permission to share these files and will rename the files so that the new file names cannot be linked to the participant’s YNiC code by researchers (without breaking the data protection policies already in place).  DPIA approval we are seeking here would cover sharing of brain data after defacing and of healthy individuals only (not including clinical research). This also only applies to research data; participants’ identifiable personal information (e.g., contact details and date of birth) cannot be publicly shared.  Furthermore, in addition to MRI data, the procedures described here, and in the default information/consent form templates provided, only cover sharing of age (years), sex, and study-specific task performance data that **do not count as special category data and that do not increase the risk of participant identification.** These study-specific task performance data (see section 3 of Table above) already fall under the responsibility of the researcher. These data can include, for instance, response times in a word recognition task or accuracy in a face perception task. If researchers want to share special category data (including data related to health) at an individual level (i.e., linked to individual participants), further approval is needed, including participant forms detailing the types of additional data to be shared and an additional study-specific DPIA. The information provided to researchers about this is attached and is also summarised as a comment in the participant form templates.  Previous DPIA approval has been provided for the following, so that a research study will not need a separate DPIA if: 1) it involves the standard initial screening procedure we outline here, 2) it uses the standard YNiC general consent form (attached), 3) it uses any of the three standard YNiC safety forms (attached), 4) the researchers  will not use any data processing techniques on pseudo-anonymised data for the purposes of  trying to determine the identity of the person from whom it was obtained, 5) researchers will not remove or copy raw data from University of York servers without following the data release application procedures and completing their own DPIA if necessary. Data that has been processed in such a way that they are no longer considered “biometric” may be copied from the University of York servers with no need for a data release application or an additional DPIA.  We are now seeking approval for an update to point 5), so that researchers can publicly share YNiC data following the procedures outlined above.  Researchers will be informed that if they use any additional health or biometric data, or if they deviate from the procedures outlined here, they will need to assess whether a study-specific DPIA is also necessary.  To determine whether a potential participant meets the safety criteria for participating in a research study, the participant may be asked any of the questions that are included in the document “**Approved questions for DPIA\_183**” (any questions that are not needed for a certain study must be removed by the researcher). It will be made clear to the individual that we need answers to these questions only if they still wish to take part, and they will be reminded that participation is purely voluntary.  If they are in doubt about how to answer a question, they can contact the researcher or YNiC for further clarification. The researcher / YNiC staff may ask necessary additional questions as part of this process. |

**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 another way of describing data flows. What types of processing identified as likely high risk are involved?** |
| 1. **Standard initial screening procedure (Stage 1 - Data collection matrix)**   Data collected: The potential participant will be asked the initial screening questions verbally or by completing a Google form. If the questions are asked verbally, the answers will be read back to the participant to ensure that errors have not been introduced. If the participant seeks further clarification from the researcher or YNiC staff, they may be asked necessary follow-up questions verbally.  Data use: Data will only be used to determine whether or not the person can take part in the research, or whether they meet the criteria for a certain experimental group or control group.  Data storage: Health data from the initial screening questions will be gathered as a Google form and stored using Google Sheets by the research team and will not be held by YNiC. The data will be stored on Google Workspace under the University’s Google Licence.  Data deletion: Google forms containing the health-related screening information will be deleted when a participant decides not to participate or when it has been decided that they do not meet the criteria for participation. If a participant meets the criteria and decides to take part, the Google form will be retained if the information may be required for data analysis. In this case, as with the imaging data, data will be held for a minimum of 10 years. Data will not be deleted unless by explicit request from the participant. It may not be possible to delete data if they are already processed and / or published - participants are made aware of this when they consent to take part in the study.  Data source: The data will come directly from the potential participant, either with the potential participant filling in the Google form, or giving verbal responses, and the researcher adding these to the Google form.  Data sharing: Health data from the screening questions may be shared with YNiC staff or other members of the research group who are internal to the University, but only in anonymised form.  High risk processing: We do not consider this data processing to be high risk.   1. **The General Consent Form  (Stage 1 - Data collection matrix) and The Safety Screening Forms.   (Stage 4 - Data collection matrix)**   Data collected: The data will be the responses given on the attached forms (one general consent form and three safety forms).  Data use: Data will be used to determine whether or not the person can take part in the research and to confirm that participants consent to their primary health care provider (usually a GP) to be contacted if an anomaly is found during scanning procedures.  Data storage: The data will be stored at YNiC.  Data deletion: Data will be held for a minimum of 10 years in a secure database. Data will not be deleted unless by explicit request from the participant.  Data source: The data will come directly from the potential participant. They will submit the general consent form to the YNiC reception and complete the safety form at YNiC.  Data sharing: The general consent form will be submitted at the YNiC reception and will only be available to YNiC staff. The participant will complete the safety form at YNiC. It will be given to the researcher/ scanner operator. After the session it will be immediately submitted to the YNiC reception where it will be stored in a locked cabinet. After that it will only be available to YNiC staff.  High risk processing: We do not consider this data processing to be high risk.   1. **Study specific information and assessments   (Stage 3 - Data collection matrix)**   Data collected: The data will be the responses given on forms and documentation related to study-specific consent and study-     specific behavioural measurements NOT held by YNiC (e.g. s     tudy-     specific consent form, study-     specific information sheet) and in digital form where outcome and results of psychological / behavioural experiment assessments are logged by      the investigator (again NOT held at YNiC).  Data use: Data will be used to (1) confirm that participants consent in general to participation in the study including procedures /  measurements / assessments carried both at YNIC (i.e. scanning) and also unrelated to YNiC specific activities (e.g. behavioural questionnaires); (2) to determine correlatable outcome values for participants from the measures that they have consented to. These data will only be used for the scientific research outcome measures declared to and approved by the ethics committee.  Data storage: The data will be stored by the investigators. Consent information will be necessarily stored in a non-anonymised format; all other behavioural / assessment information relating to any individual participant will be stored with reference to their pseudo-anonymised ID only.  Data deletion: As with the imaging data, data will be held for a minimum of 10 years. Data will not be deleted unless by explicit request from the participant. It may not be possible to delete data if they are already processed and / or published - participants are made aware of this when they consent to take part in the study.  Data sharing: These data might be shared publicly by researchers in combination with MRI data, but (under this DPIA and following the default participant forms) only if they do not increase the risk of participant identification and if they do not count as special category data. Sharing of special category behavioural data in combination with the MRI data requires further approval and a study-specific DPIA.  4) Storage of Imaging data (that may allow reconstruction of **potentially sensitive biometric data -   (Stage 5 - Data collection matrix)**  Data collected: The data collected during routine data acquisition techniques used at YNiC - MRI, MEG and TMS - have the potential to reveal “biometric data” from an individual participant’s pseudo-anonymised data if a person with access to such data were (1) inclined to deliberately attempt to reconstruct the data to reveal biometric measures and (2) if the person attempting to unmask the biometric data has access to an appropriate reference dataset for the participant.  Data use: This data will be used for research purposes. All researchers and staff who have access to the centre will sign the YNiC Appropriate  Data Usage Declaration when they register to have access to data stored at YNiC (NB - all active users of the centre will have to sign this declaration retrospectively if they are currently using the center, both for newly acquired data and data acquired in the past). As part of the ethics process it will be made clear to researchers that they must not use the data in any way to attempt to unmask the identity of any individual pseudo-anonymised participant.  Data storage: The data will be stored on University of York IT systems in pseudo anonymised format.  Data deletion: Data will be held for a minimum of 10 years in a secure database. Data will not be deleted unless by explicit request from the participant. It may not be possible to delete data if they are already processed and / or published - participants are made aware of this when they consent to take part in the study.  Data source: The data will come directly from the participant during the data acquisition procedures at YNiC.  Data sharing: When completing their training prior to using YNiC facilities, it will be made clear to researchers that if wish to share any data outside of the organisation they must (1) seek approval from the ethics committee in advance and (2) must do this in a way that does not allow others to reconstruct biometric data that could be used to reveal the identity of an individual participant’s data from that participant’s pseudo-anonymised data set.  To share data openly, for example in a repository, and for that to be covered by the updated DPIA\_183, the following conditions must be met:  1) participants must have signed the updated consent form (version number 9)  2) the scan data must be defaced,  3) the participants must not be labelled as belonging to a certain group (e.g., clinical groups). This does not apply to groups defined by age or sex (see point 4),  4) there must be no other data shared with the brain data except for age and sex. Task performance data can only be shared with the brain data if they are not sensitive (special category data, including data providing information about physical or mental health) and/or do not increase the risk of identifying a participant.  When researchers are sharing data as part of a collaboration, they will also need to work with the University’s Research and Knowledge Exchange Contracts Team to ensure an appropriate agreement is in place (eg. a Memorandum of Understanding to cover Intellectual Property etc.  High risk processing: We do not consider this data processing to be high risk. |
| **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 nature of the “special category” health and potentially biometric data is described in step 1 above.  Step 1 also outlines how much health data will be collected / used. The MR, TMS and MEG data are  not intrinsically “biometric” (according to the definition provided in the Glossary of the University’s Records Management & Information Governance webpage in October 2021) and it will be made clear to researchers that they must not process the data in such a way that would make it fall into this category. Specifically, none of the pseudo-anonymised stored on University of York IT systems should be used in such a way to deliberately attempt to ascertain the identity of the participant from whom those data were collected.  The standard initial screening procedure will be completed at the start of each study (Stage 1). The general consent form is usually completed once, before the participant takes part in any research at YNiC (Stage 2) . The safety questions are completed each time a participant arrives at YNiC to take part in research (which may be multiple times during the course of their participation in a certain research study) (Stage 4).  The Google form containing health data from the screening questions will be deleted if a participant does not meet the criteria to take part in the research or if they decide not to participate. If they do decide to participate, data from the screening questions and general consent form will be kept indefinitely, or until the participant asks for it to be removed. Data from the safety forms will be kept indefinitely so there is a record of the safety screening procedure that took place.  This affects everyone who participates in research approved by the YNiC Research Ethics Committee. Participants may be from anywhere in the world. They may be excluded from participating in the research for reasons relating to safety or study-specific requirements, not geographical area (unless this is a study-specific requirement). |
| **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?** |
| Potential participants may be individuals who are seeking the opportunity to take part in research (eg. they asked to join the YNiC research database, they have found the research study advertised on the SONA participant pool, they have responded to a poster or email asking for research volunteers).  Participants are in complete control over whether or not they share their “special category” health data. It will be made clear to the individual that we need answers to these questions only if they still wish to take part, and they will be reminded that participation is purely voluntary. They will also be told that the data will only be used to establish whether or not it is safe for them to participate in the research, and if they belong to a population of interest for the research. Specific studies might collect additional special category data (step 3), which fall under the researchers’ responsibility and can only be shared with the participants’ permission and with an additional study-specific DPIA. Together with the information sheet (which they will receive prior to any data being collected) participants will be issued with a GDPR compliant privacy notice, using the template from the University’s Records Management and Information Governance, Data Protection webpage, accessed in January 2022.  The participants may include children or vulnerable groups. When a participant is under the age of 16 and/or lacks the capacity to consent, the consent forms are completed on their behalf and signed by their legal guardian.  We are not aware of any prior concerns over this type of processing, or the technology used, of any security flaws or of any current issues of public concern that should be factored in. These procedures are very well established at YNiC. |
| **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?** |
| For the health data: As stated in Step 1 above, we want to achieve 1) a decision about whether it is safe for that person to participate in the research and 2) a decision about whether that person belongs to a population of interest for the research.  From completing this processing we will be able to provide the participant with a decision on whether or not they can participate in the research. We will also be able to compare data from participants from different populations of interest (eg. patients compared to healthy controls).  For the potentially biometric data: this is not relevant because the data will not exist in a format that may be classed as “biometric”.  Intended effects will vary study to study. However, all studies will receive ethical approval. |

**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?** |
| YNiC staff or other members of the research team may be consulted to establish whether or not a person can participate in the research, but if this is needed then the health data will be anonymised. This may involve asking the potential participant additional questions, but again it will be made clear to the participant that they are under no obligation to provide this additional information.  These procedures are well established at YNiC so there is no need to consult information security experts etc.  Before each project can begin there will also be consultation with the ethics committee (as part of the standard application procedure) to ensure that the study-specific data the researchers wish to collect is appropriate. Note that this DPIA covers only the five stages outlined in Step 1 above. The ethics committee will assess all other aspects of proposed projects in the normal way. |

**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?** |
| 1. **Standard Initial Screening Procedure**   An alternative approach would be to ask potential participants to scan a list of criteria to determine for themselves whether they meet the criteria. However, this may not achieve the same outcome as asking participants to engage with each question. It is important that participants engage with each question so that we can make an accurate assessment about whether or not they can participate prior to them arriving at the YNiC to take part in the research. Making an accurate assessment in advance means that they are less likely to discover that they cannot be scanned when they are filling in the safety form at YNiC, immediately prior to the scheduled research session. If a participant discovers that they cannot be scanned when they are filling in the safety form at YNiC, they will have had a wasted journey and the researcher will have to pay for unused scan time.  Individual researchers will remove questions that do not apply to their study. Data quality will be ensured as the potential participants will provide the information themselves.  When given the initial screening questions, participants will be informed:  *“Magnetic Resonance (MR) research takes place in a strong magnetic field. Therefore, no metallic items can be taken into the scanner since they will get attracted by the magnet. They may also be heated up by the radio waves. For the same reason, people with metallic implants or other items cannot be scanned. There may be other reasons why a person cannot take part in the research. For example, we may need certain people to be able to answer our specific research questions. If you wish to take part in the research, we need answers to the following questions so we can establish whether or not you can take part in the research. Please remember that participation is purely voluntary. “*  Ethical approval for research at YNiC will be granted on the condition that these procedures are adhered to.     1. **The General Consent Form and 3) The Safety Forms.**   The questions in the general consent form and the safety forms are necessary and sufficient to establish whether a participant can take part in the research.  These are well-established procedures at YNiC. The data comes directly from the participant, ensuring its quality and we ask very specific and necessary questions (see the attached forms), ensuring data minimisation.  Prior to conducting any research at YNiC a researcher must complete safety training, which includes training in these procedures. Ethical approval for research at YNiC will also be granted on the condition that these procedures are adhered to.  **Potentially biometric data:**  Ethical approval for research at YNiC will be granted on the condition that data are not used or processed in such a way that they are being used to unmask the subject’s identity from their individual pseudo-anonymised data and that data which could be used to reconstruct such information will not be shared outside of the organisation. Under this revised DPIA and following the default participant forms, MRI data can only be shared publicly after defacing and after renaming of the files, ensuring very low risk of identification. |

**Step 5: Identify and assess risk**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk no.** | **Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.** | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
|  | | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |
| 1 | If the standard initial screening procedure is not followed correctly, or if the Google form is accessed by someone outside of the research team, health information, together with identifying information, may become available to others. | Remote | Significant | Low |
| 2 | It is technically possible that if anonymised health information needs to be shared to establish whether or not a person can take part, there might be enough of that information for it to no longer be considered anonymous. However, this information will only be shared with trained YNiC staff or the PI, so there is unlikely to be any impact on individuals. | Remote | Minimal | Low |
| 3 | If the outlined procedures are not followed correctly, or if YNiC data security is compromised, personal health information from the general consent form and the safety forms may become available to others. | Remote | Significant | Low |
| 4 | If the outlined procedures are not followed correctly, or if University of York data security is compromised, it is possible that a representation of the participant’s face may be constructed from their MR data. | Remote | Significant | Low |
| 5 | There is a risk that too much data will be collected. | Remote | Minimal | 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 or accepted | Eliminated, reduced or accepted | Yes/no |
| 1 | Documented procedures will be maintained and all staff will receive training to ensure best practice is followed. | Reduced | Reduced | Yes |
| 2 | Whilst this is possible, at all times the minimum amount of data necessary is gathered. In addition, any individual provided access to identifiable data is bound by University contract and subject to existing information policies and regulations. | Reduced | Reduced | Yes |
| 3 | Robust arrangements are in place to ensure documented procedures are followed. In addition, all staff have received training on data protection and information security. | Reduced | Reduced | Yes |
| 4 | As 3 above. | Reduced | Reduced | Yes |
| 5 | However, having a standard set of safety screening questions and ensuring that the ethics committee check the study-specific questions prior to giving ethical approval should ensure that researchers collect the minimum amount of data needed. | Reduced | Reduced | Yes |

**Step 7: Sign off and record outcomes**

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/date** | **Notes** |
| Measures approved by: | Durham Burt, DPO, 31 March 2022  v2 submitted for review 5 May 2023. Approved 5 July 2023.  v3 submitted for review 20 October 2023. Approved 20 October 2023. | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: | Durham Burt, DPO, 31 March 2022  v2 residual risk  unchanged.  v3 residual risk unchanged. | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: | Yes, at the point of DPIA submission. | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice:  *Provided the mitigations outlined in this DPIA are fully adopted, risk arising from this arrangement will be low. This DPIA should, of course, be kept under review and should be revisited in the event a change to the arrangement is envisaged e.g., a new use for data identified or a proposal to substantially deviate from current arrangements is proposed.* | | |
| DPO advice accepted or overruled by: | Accepted  by Fiona McNab,  Chair of Ethics YNiC Research Ethics Committee | If overruled, you must explain your reasons |
| Comments: None. | | |
| Consultation responses reviewed by: | N/A | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: N/A | | |
| The DPIA will be kept under review by: | Fiona McNab,  Chair of Ethics YNiC Research Ethics Committee and Andre Gouws,  Operations Manager | The DPO should also review ongoing compliance with DPIA |

Source: Information Commissioner’s Office, *DPIA Template, available,* <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>.