DPIA Form

Completed By	Jenny Wheeldon	**23/02/2024**	
Department	HSR UK		

Project Title:	Careers Inclusion

Step1: Explain the project in broad terms

1.1. What are the aims and objectives of the data processing? - Why was the need for a DPIA identified?

Aims and objectives:

1) To provide demographic data to both map representation within the existing health and social care services research workforce and inform us as to whether this is an adequately representative sample or whether research needs to be expanded beyond this community.

2) To understand the backgrounds, career entry points/histories/trajectories and experiences of career pathways and problems health and social care services researchers have faced/encountered.

3) Identify what works well with the current system and what could be developed,

The need for a DPIA was identified due to the sensitive data and protected characteristics that will need to be collected in order to meet the above research objectives.

Step2: Describe the processing

2.1. Describe the information flow: 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?
Survey data flow Step 1: respondent completes survey (survey developed using Microsoft Forms application) and creates the data Step 2: submitted survey data is stored on HSR UK's Microsoft 365 Microsoft Forms app (login/password protected to HSR UK team only) Step 3: survey data from multiple respondents will be exported from Microsoft Forms app to Excel spreadsheets, which will then be stored on HSR UK OneDrive (also login/password protected to HSR UK team only) Step 3: Excel spreadsheets containing curated survey data may be shared with external partners to assist with statistical data analysis. Partners will include: members of the project advisory group which includes contacts from academic institutions and NIHR, HSR UK board trustees and contracted research associates. Note: external partners will not have direct access to the data and data source (e.g. Microsoft Forms or HSR UK OneDrive) Step 4: Data will be used for output report(s) and may include direct quotations from qualitative survey questions - in such cases, quotations will be identified by the respondent's job title only Step 5: upon completion of the project (currently scheduled as April 2026) exported Excel spreadsheets containing the data will continue to be be stored securely via OneDrive for two years and after this time will be subject to risk assessment as is stipulated in HSR UK's privacy notice. Data stored though the Microsoft Forms app will be deleted upon completion of the project. The highest risk associated with the processing of this data is the sharing of curated data with external partners.

Data Flow Diagram / Location	N/A
(Upload file or provide link)	N/A

2.2. 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?

Although data collected does not include directly identifiable information (e.g. names, contact details) we are planning to collect demographic data including protected characteristics. A previous HSR UK survey had 250 respondents although not all surveys were complete. With this mind and due to the topic, we plan to collect data from 100 individuals at which point we will assess data saturation. Initially, the survey will be open for 30 days with the option to extend to 60 days should recruitment levels be lower than anticipated. This is a national survey for England, Wales, Scotland, Northern Ireland and Ireland.

2.3. 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)?

Nature of relationships with survey participants: part of the health services research community

Control of survey participants: throughout the survey form, multiple choice questions offer the option 'prefer not to say' and open-ended questions promote the option to type 'N/A' or 'prefer not to say'; survey respondents are therefore in control of which data they choose to share. The survey introduction also states that all questions are optional to answer. Due to not collecting contact information, once data is submitted through the survey it will not be possible to retrieve/remove individuals' data. This is stated in HSR UK's updated privacy policy.

Type of survey participants: professionals (no children or vulnerable populations)

2.4. Describe the purpose 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?

From processing the data, we plan to achieve the previously stated research objectives. This is the first step to identifying issues within this topic area and ultimately working towards improving career difficulties for the research community (i.e. the survey respondents).

Data processing benefits HSR UK by providing us with valuable information regarding the researcher community which will inform interventions to improve career experiences for specific groups; this will form Phase Two of the Careers Inclusion project and therefore, the data collected and processed from the survey is integral to the overall success of the project. Completing this work will also provide valuable research experience and strengthen HSR UK's organisational capacity to carry out future research activities and projects. Published material informed by the data (i.e. output reports) will also be useful to promote HSR UK and create further opportunities to collaborate with partners and organisations.

Step 3: Consultation process

3.1. 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 plan to consult IT (e.g. to set up Secure File Transfer), or IG (to draw up data sharing agreements)?

We plan to consult with both IT and IG if and when the need to share curated data files with external partners/stakeholders for the purpose of data analysis arises. Note: direct access to data/"raw" data will be limited to the HSR UK team only and any data shared with external partners will be curated to ensure only the necessary data is shared for the specific purpose of the data analysis in question. External partners will include project advisory boards, HSR UK trustees and contracted research associates.

Step4: Assess necessity and proportionality

4.1. 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?

In order to meet the research objectives, we must collect the described data. Several stages of consultation have been completed for the design of the survey to ensure data quality and data minimisation. As data processing will be completed solely by the HSR UK team, all team members are aware of internal data processing practices and are up to date with data protection and other relevant training.

Step 5: Identify and assess risks

Describe 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**
1. Users or administrators may deliberately steal or release data from the processing environment.	**Remote**	**Significant**	**Low**
2. The IT service Third party providers/contractors accidentally or deliberately removes data from the processing environment.	**Remote**	**Significant**	**Low**
3. A physical intruder could steal equipment related to the processing environment.	**Remote**	**Significant**	**Low**
4. External (Internet) hackers breach external defences and gain access to the data folders, resulting in theft or release of data.	**Remote**	**Significant**	**Low**
5. A hacker within wireless range could breach the wireless network and gain access to data.	**Remote**	**Significant**	**Low**
6. Sensitive Research Data is accidentally transferred from the restricted data folders.	**Remote**	**Minimal**	**Low**
7. Unauthorised Access to data	**Remote**	**Significant**	**Low**
8. Insufficient security measures applied to IT Systems	**Remote**	**Severe**	**Low**

9. Firewall allows internet access to research folders	**Remote**	**Severe**	**Low**
10. There is limited or no management control or oversight	**Remote**	**Severe**	**Low**
			#N/A
			#N/A
			#N/A
			#N/A
			#N/A
			#N/A
			#N/A
			#N/A
			#N/A

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
1	1. Ensure users training is adequate 2. Ensure procedures make accidental loss unlikely 3. Remote Working Guidelines	Reduced	Low	Yes
2	1. Monitor compliance with Policy and procedures 2. Confidentiality agreement sets out user obligations	Reduced	Low	Yes
3	1. Ensure physical security measures are adequate to prevent intrusion, or detect break-ins quickly. 2. ACL Policy applied 3. Encryption (AES 256 bit) applied to data folders and backups	Reduced	Low	Yes
4	1. Confirm that boundary controls are effective 2. Limit exposed services 3. Regular penetration testing	Reduced	Low	Yes

5	1. Ensure the wireless configuration is robust 2. Seek independent validation (as part of penetration testing)	**Reduced**	**Low**	**Yes**
6	1. IG Training 2. System and file auditing 3. File filtering through firewall	**Reduced**	**Low**	**Yes**
7	1. Access Control Policy 2. Physical Security Policy 4. Data Encryption	**Reduced**	**Low**	**Yes**
8	1. Security documentation 2. Implementation of Security Policies	**Reduced**	**Low**	**Yes**
9	1. Acceptable Use of Internet Policy 2. Patch Management Policy 3. Firewall Configuration Rules 4. Penetration Testing	**Reduced**	**Low**	**Yes**
10	1. Security documentation 2. Data Strategy Group (DSG) 3. Leadership Team (LT) 4. IG Training	**Reduced**	**Low**	**Yes**

Step 5: Sign Off And Record Outcomes

7. Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.

Item	Name / date	Notes
Approved by:	Jenny Wheeldon, 26/2/24	Integrate actions back into project plan, with date and responsibility for completion
Residual Risks approved by:	Cat Chatfield, 26/2/2024	If accepting any residual high risk, consult the ICO before going ahead
DPO Advice Provided:	Tony Harbon, 23/2/2024	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO Advice		

DPO advice accepted / overruled by:	Cat Chatfield, 26/2/2024	Reasons must be given if DPO advice is overruled
Comments		