Reviewer's Rubric for Data Management Plans v 1.0 May 2024

DMP Question	DMP Guidance	Sufficiently Addressed	Insufficiently Addressed
1. Description of the data			
1.1 Type of study	Up to three lines of text that summarise the type of study (or studies) for which the data are being collected.	Clearly summarises the type(s) of study.	Does not clearly summarise the type(s) of study.
1.2 Types of data	Types of research data to be managed in the following terms: quantitative, qualitative; generated from surveys, clinical measurements, interviews, medical records, electronic health records, administrative records, genetic and genomic data, images, tissue samples, code, software and workflows etc.	Clearly describes or lists what types of research data will be managed (for example numeric, textual, audio, video, software, workflows etc.) or provides a valid reason for omitting these details.	Provides no or little details on what data types will be managed and does not provide a valid reason for this omission.
1.3 Format and scale of the data	File formats, software used, number of records, databases, sweeps, repetitions, etc. (in terms that are meaningful in your field of research). Indicate the size of data to be stored and made available. Do formats and software enable sharing and long-term validity of data?	Clearly explains why certain formats have been chosen and indicates if they are in open and standard format. If a proprietary format is used, it explains why. Provides information about the estimated data size and/or volume. Clearly explains how formats and software chosen enable sharing and long-term validity of data.	Only lists/describes the kinds of data without specifying their formats. Only lists formats, without specifying the kinds of data. Does not provide an estimate of data size or volume. Does not mention how formats and software chosen will enable sharing and long-term validity of data.

DMP Question	DMP Guidance	Sufficiently Addressed	Insufficiently Addressed
2. Data collection / generation Applicants are asked to justify why new data collection or long-term management is needed in their Vision and Approach sections. In this section, applicants are expected to focus on the good practice and standards they will use for ensuring new data are of high quality.			
2.1 Sources of data	Will you be collecting/ generating new data or re-using existing data? And how will you achieve this?	Gives clear details of where the existing data come from and how new data will be collected or produced. It clearly explains methods and software used. Explains, if existing data are re-used, how these data will be accessed and any constraints on their re-use. Explains clearly, if applicable, why new data must be collected, rather than re-using existing data.	Provides little or no details on where the data come from and what data will be collected or re-used. Does not, if applicable, provide sufficient rationale for generating new data.
2.2 Data quality and standards	Which community data standards (if any) will be used at this stage? How consistency and quality of data collection / generation will be controlled and documented, through processes of calibration, repeat samples or measurements, standardised data capture or recording, data entry validation, peer review of data or representation with controlled vocabularies.	Clearly describes the approach taken to ensure and document quality control in the collection of data during the lifetime of the project.	Provides no information or only a vague mention on how data quality is controlled and documented during the lifetime of the project.
2.3 Consent for data sharing and re-use	If you are obtaining consent or consent has been obtained previously, please explain how this allows data sharing and re-use.	Consent for data sharing has been achieved and recorded.	Consent for data sharing has not been achieved.

DMP Question	DMP Guidance	Sufficiently Addressed	Insufficiently Addressed
3. Data management, documentation and curation Applicants are expected to focus on principles, systems and major standards to enable data to be FAIR.			
3.1 Managing, storing and curating data	Briefly describe how data will be stored, backed-up, managed and curated in the short to medium term. Specify any community agreed or other formal data standards used (with URL references) to enable interoperability.	Clearly describes the location where the data and backups will be stored during the research activities, how often backups will be performed, the use of robust, managed storage with automatic backup (for example storage provided by the home institution).	Provides no information or very vague reference to how data will be stored and backed up during the project.
3.2 Metadata standards and data documentation	What metadata is produced about the data generated from the research? For example, descriptions of data that enable research data to be used by others outside of your own team. This may include documenting the methods used to generate the data, analytical and procedural information, capturing instrument metadata alongside data, documenting provenance of data and their coding, detailed descriptions for variables, records, etc.	Clearly outlines the metadata that will accompany the data, with reference to good practice in the community (for example uses metadata standards where they exist). Clearly outlines the documentation needed to enable data re-use, stating where the information will be recorded (for example a database with links to each item, a 'readme' text file, file headers, code books, or lab notebooks). Indicates how the data will be organised during the project (for example naming conventions, version control strategy and folder structures).	Provides little or no details on the metadata that will accompany the data. Provides no information, or only a very vague mention of documentation, without providing any detail or explanation.

DMP Question	DMP Guidance	Sufficiently Addressed	Insufficiently Addressed
3.3 Data preservation strategy and standards	Plans and place for long-term storage, preservation and planned retention period for the research data. Include formal preservation standards, if any. Indicate which data may not be retained (if any).	Provides details of what data collected or created in the project will be preserved in the long term and clearly indicates for how long. This should be in alignment with funder, institutional, or national policies and/or legislation, or community standards. Provides details of which (versions of) data and accompanying documentation will be retained or destroyed, and explains the rationale (for example contractual, legal requirements, or regulatory purposes), how these will be archived in the long term and provides the name of the archive or trustworthy repository – or the way to curate and preserve data – that will be used to make data available for re-use.	Provides no further information or lacks adequate explanation on what provisions would be made for data preservation.

4. Data security and confidentiality

Sections 4 and 5 have been updated in April 2024 to include consideration of safe and secure international collaboration in line with the UKRI Trusted Research and Innovation Principles.

Applicants are asked to complete this section if any of the below is relevant:

- their data includes data relating to human participants
- their proposal involves international collaborations
- data related to sensitive areas might be shared with, or access given to individuals and organisations overseas
- other research, for which the safeguarding and security of data should be considered

DMP Question	DMP Guidance	Sufficiently Addressed	Insufficiently Addressed
4.1 Formal information/data security standards	Identify formal information standards with which your study is or will be compliant. An example is ISO 27001.If your organisation is ISO compliant, please state the registration number.	Clearly explains which formal information standards (such as institutional and/or national data protection policies) are in place and provides a link to where they can be accessed.	Provides little or no details of formal information standards, if applicable.
4.2 Main risks to data security and how they will be managed	Please summarise the risks specific to your research that would require data security measures to be implemented. This should include: • risks to the confidentiality and security of data and information • risks of misuse and describe the level of risk and how these risks will be managed. Cover the main processes or facilities for storage and processing of personal data, data access, with controls put in place and any auditing of user compliance with consent (where applicable) and security conditions. **It is not sufficient to write <u>not applicable</u> under this heading.** If you intend to work with overseas collaborators or data users, describe how your approach ensures that the team has a robust cyber-security culture and a process to identify and protect any sensitive data and information. Further guidance is available on the MRC Data Management and Sharing page and the UKRI principles and guidance on trusted research and innovation.	Clearly explains who will have access to the data during the research. Clearly explains how the data will be recovered in the event of an incident. Clearly describes the additional security measures (in terms of physical security, network security, and security of computer systems and files) that will be taken to ensure that stored and transferred data are safe, when sensitive data are involved (for example personal data, security-sensitive information, or trade secrets). Clearly identifies levels of risk and provides solutions to effectively manage these. Clearly states the processes put in place to ensure a robust cyber-security culture and to identify and protect any sensitive data and information, when working with overseas collaborators or data users.	Provides little or no details on who will have access to the data during the research. Provides little or no details on how the data will be recovered in the event of an incident. Provides little or no details about data protection and risk management, or the explanation is too vague, when sensitive data are involved (for example personal data). Provides little or no details about processes put in place to ensure a robust cyber-security culture and to identify and protect any sensitive data and information, when working with overseas collaborators or data users.

DMP Question	DMP Guidance	Sufficiently Addressed	Insufficiently Addressed
5. Data sharing and access Applicants are expected to identify any data repository or repositories that are, or will be, entrusted with storing, curating and/or sharing data.			
5.1 Suitability for sharing	Is the data you propose to collect in the study suitable for sharing within the team and with external users (including international)? If yes, briefly state why it is suitable and explain how risks, such as re-identification will be managed. If you are re-using data, what steps will you take to ensure further sharing of the data? If no, indicate why the data will not be suitable for sharing and then go to Section 6.	Clearly describes what new or re-used data is suitable for sharing, what possible interest there would be for re-use (or not) and explains how risks, such as re-identification will be managed.	Provides no further information or lacks adequate explanation on what provisions would be made for data sharing.
5.2 Discovery by potential users of the research data	Indicate how potential new users (outside of your organisation) can find out about your data and identify whether it could be suitable for their research purposes. This can be done through making summary information (metadata) readily available on the study website, in the HDRUK Gateway, or in other recognised databases or catalogues. How widely accessible is this repository? How will you make your data FAIR, including sharing necessary methods or software tools to access it? Indicate whether your policy or approach to data sharing is (or will be) published on your study website or otherwise accessible. Will unique and persistent identifiers be attributed to your data, methods, or software to allow data users to cite them and data generators to track them?	Clearly describes how and when the data and/or metadata will be made discoverable and specifies under which licence. Includes the name of the repository, data catalogue, or registry where data will or could be shared. Clearly indicates which specific tools or software (for example specific scripts, codes, or algorithms developed during the project, version of the software) potential users may need to access, interpret, and (re-)use the data.	Provides little or no details on how, when and where data will be shared. Provides little or no details on which software developed during the project will be necessary to access and interpret the data, how it will be made available, or why that may not be possible. Makes no mention of PIDs nor provides a valid reason for not providing them.

DMP Question	DMP Guidance	Sufficiently Addressed	Insufficiently Addressed
		Clearly indicates where information on data sharing will be published. Clearly indicates if and which persistent identifiers (PIDs) are provided for all datasets, individual datasets, data collections, or subsets. If PIDs will not be used, it explains why.	
5.3 Governance of access	Identify who makes or will make the decision on whether to supply or grant access to research data to a potential new user. For population health and patient-based research, indicate how independent oversight of data access and sharing works (or will work) in compliance with MRC policy and guidance. Explain whether you will have a public data release register with information about sharing. Indicate whether the research data will be deposited in and available from an identified community database, repository, archive or other infrastructure established to curate and share data.	Provides information on any protocol to access the data (for example if authentication is needed or if there is a data access request procedure) and who will be responsible for supplying the data to a potential new user. Indicates how compliance with MRC policy will be achieved for population health and patient-based research. Includes the name of the community database, repository, archive or other infrastructure where data will be shared.	Provides little or no details on who will be supplying research data to potential new users, and where the data will be shared (such as a repository or other infrastructure). Does not provide any information on how compliance with MRC policy will be achieved for population health and patient-based research.
5.4 The study team's exclusive use of the data	MRC's requirement is for timely data sharing, with the understanding that a limited, defined period of exclusive use of data for primary research is reasonable according to the nature and value of the data, and that this restriction on sharing should be based on simple, clear principles. What are the	Specifies when data will be shared and under which licence. Includes information on how long the data will be retained and gives precision on its timely release.	Provides little or no details on how and when data will be shared.

DMP Question	DMP Guidance	Sufficiently Addressed	Insufficiently Addressed
	timescale/dependencies for when data will be accessible to others outside of your team? Summarize the principles of your current/intended policy.		
5.5 Restrictions or delays to sharing, with planned actions to limit such restrictions	Restriction to data sharing may be due to participant confidentiality, consent agreements or IPR. Strategies to limit restrictions may include data being anonymised or aggregated; gaining participant consent for data sharing; gaining copyright permissions. For prospective studies, consent procedures should include provision for data sharing to maximise the value of the data for wider research use, while providing adequate safeguards for participants. As part of the consent process, proposed procedures for data sharing should be set out clearly and current and potential future risks associated with this explained to research participants.	Clearly explains, if applicable, why data sharing is limited or not possible, and who can access the data under which conditions. Explains, where possible, what actions will be taken to overcome or to minimise data sharing restrictions. Clearly explains that the consent procedure includes provision for data sharing.	Provides little or no details about why data sharing might be limited or what actions will be taken to overcome data sharing restrictions. Consent procedure does not include provision for data sharing.
5.6 Regulation of responsibilities of users	Indicate whether external users are (will be) bound by data sharing agreements, setting out their main responsibilities.	Clearly describes who will be able to use the data, and if it is necessary to apply a data sharing agreement which sets out users' responsibilities.	Does not provide any information on data sharing agreement or users' responsibilities.
5.7 Working with overseas collaborators or data users	Please indicate how sensitive data will be shared with international collaborators and/or accessed by overseas data users. Describe measures to manage associated risks. Have you considered legislation of overseas partners that might permit authorities to access sensitive information without consent from all	Clearly states the processes put in place to ensure a robust cyber-security culture and to identify and protect any sensitive data and information, when working with overseas collaborators or data users. Includes consideration of relevant legislation of overseas	Provides little or no details on how sensitive data will be shared with international collaborators. Does not include any information on relevant legislation of overseas partners.

DMP Question	DMP Guidance	Sufficiently Addressed	Insufficiently Addressed
	parties? If yes, please comment on how you will respond to this potential risk. If applicable, describe what measures you will put in place when sharing data, and how you will comply with UK's export control legislation and any other legal requirements, as per UKRI's Trusted Research and Innovation Principles and UK government guidance (National Protective Security Authority's Trusted Research Guidance for Academia and Industry). For more information follow this link.	partners that might have an impact on access to data. Clearly describes evidence of compliance with UK's export control legislation and any other legal requirements.	Provides little or no evidence of compliance with UK's export control legislation and any other legal requirements.
6. Responsibilities			
6.1 Responsibilities	Apart from the PI, who is responsible at your organisation/within your consortia for: • data management • metadata creation • data security • quality assurance of data • implementation and maintenance/ revision of DMP	Clearly outlines the roles and responsibilities for data management (for example data capture, metadata creation, data security, data quality, storage and backup, data archiving, and data sharing), naming responsible individual(s) where possible. Clearly indicates who is responsible for day-to-day implementation and adjustments to the DMP.	Does not discuss responsibility for data management activities and/or does not indicate who is responsible for day-to-day implementation and adjustments to the DMP.
7. Relevant policies			
7.1 Relevant institutional, departmental or study policies on data sharing and data security	Please complete, where such policies are (i) relevant to your study, and (ii) are in the public domain, e.g. accessible through the internet. Add any others that are relevant	Includes relevant institutional, departmental or study policies on data sharing and data security.	Provides little or vague mentions of relevant institutional, departmental or study policies on data sharing and data security.