



Policy Guidelines on Open Science & Open Data: Envisioning Open Science Road Map for RESPIRE Project Partner Countries

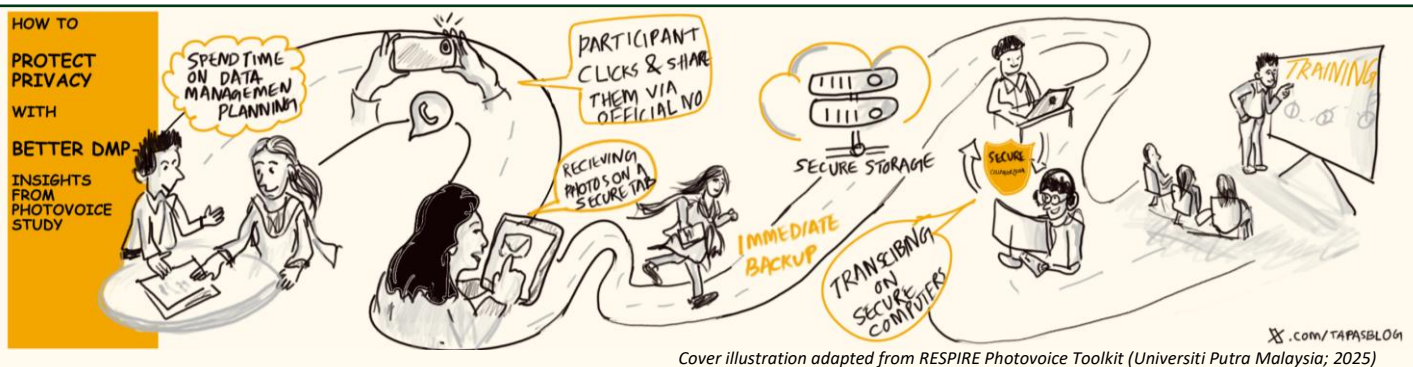
This document includes details taken from the data protection bills and acts of seven RESPIRE LMICs and addresses safeguarding sensitive information and ensuring the privacy and security of research participants involved in the research process.

Version 1

Jul, 2026

Tapas Kumar Mohanty, Informatics and Data Science Liaison Officer, NIHR Global Health Research Unit on Respiratory Health (RESPIRE), The University of Edinburgh; King George's Medical University, Lucknow, India

Simon Smith, Research Data Support Officer, Library & University Collections, The University of Edinburgh.



Cover illustration adapted from RESPIRE Photovoice Toolkit (Universiti Putra Malaysia; 2025)

The NIHR Global Health Research Unit on Respiratory Health (RESPIRE) is funded by NIHR 16/136/109 and NIHR132826 using UK international development funding from the UK Government to support global health research. The views expressed in this publication are those of the author(s) and not necessarily those of the NIHR or the UK government.

Led by:



THE UNIVERSITY
of EDINBURGH



UNIVERSITI
MALAYA

FUNDED BY

NIHR

National Institute for
Health and Care Research



UK International
Development
Partnership | Progress | Prosperity



Policy Guidelines on Open Science & Open Data:

Envisioning Open Science Road Map for RESPIRE Project Partner Countries

This document includes details taken from the data protection bills and acts of seven RESPIRE LMIC and addresses safeguarding sensitive information and ensuring the privacy and security of research participants involved in the research process.

V-1.0, Jul 2026

Tapas Kumar Mohanty

Informatics and Data Science Liaison Officer, NIHR Global Health Research Unit on Respiratory Health (RESPIRE), The University of Edinburgh; King George's Medical University, Lucknow, India

And

Simon Smith

Research Data Support Officer, Library & University Collections, The University of Edinburgh.

NIHR Global Health Research Unit on Respiratory Health (RESPIRE)



First published in 2026 by The University of Edinburgh

<https://books.ed.ac.uk/edinburgh-diamond> | [@EdinDiamond](#)

Text © Tapas Kumar Mohanty and Simon Smith, 2026

Images © Copyright holders named in captions

The authors have asserted their rights under the Copyright, Designs and Patents Act 1988 to be identified as the authors of this work.



This book is published under a Creative Commons Attribution 4.0 International license (CC BY 4.0), unless otherwise stated. This license allows you to share, copy, distribute, and transmit the work, as well as adapt and build upon it, for any purpose, even commercially, provided that appropriate credit is given to the original author(s).

<https://creativecommons.org/licenses/by/4.0/>

Attribution should include the following information:

Tapas Kumar Mohanty and Simon Smith. 2026. *Policy Guidelines on Open Science & Open Data: Envisioning Open Science Road Map for RESPIRE Project Partner Countries*. Edinburgh: The University of Edinburgh. <https://doi.org/10.2218/ED.9781836450764>

Any third-party material in this book is not covered by the book's Creative Commons license. Details of the copyright ownership and permitted use of third-party material is given in the image credit lines. If you would like to reuse any third-party material not covered by the book's Creative Commons license, you will need to obtain permission directly from the copyright owner.

ISBN (ebook): 978-1-83645-076-4

DOI: 10.2218/ED.9781836450764

DOI link: <https://doi.org/10.2218/ED.9781836450764>

Cover design: Adapted from the RESPIRE Photovoice Toolkit (Universiti Putra Malaysia, 2025)

Back cover illustration by: Tapas Kumar Mohanty

Formatted by: Kitty Flynn

Acknowledgements

We would like to express our gratitude to the following individuals and organisations for their invaluable contributions to drafting this Open Science Policy Guidelines:

1. Mentors and Advisors:

- Prof. Harry Campbell, Prof. Ee Ming Khoo, Prof. John Norrie, Prof. Sanjay Juvekar, Dr Ruth McQuillan and Dr Anand Kawade for their mentorship, guidance and insightful feedback throughout the drafting of the policy document.
- Tathagata Bhattacharjee for his encouragement and expertise in Open Science.

2. Collaborators and Colleagues:

- Dr Dhiraj Agarwal and Ms Uddhavi Kand, for sharing some insights from the Global perspective along with the local context of Vadu HDSS.
- Professor Sajid Soofi, Imran Ahmed Chauhadry, Dr Amina Khan, Mr Naresh Singh, Prof. Cheong Ai Theng, Samina Huque, Asiful Chowdhury, Fahmidur Rahman, SH Rana and Dr B M G Duminda Yasaratne for their valuable input and support.

3. Funding and Support:

- This research was funded by NIHR 16/136/109 and NIHR132826 using UK international development funding from the UK Government to support global health research. The views expressed in this publication are those of the author(s) and not necessarily those of the NIHR or the UK government.
- RESPIRE Collaboration, for administrative and logistical support.

4. Family and Friends:

- Gudi Nepak and Rati Ranjan Senapati, thank you for your unwavering support and understanding during the drafting.

5. Special Thanks:

- Kitty Flynn, for her exceptional contribution in formatting and tweaking the document in line with the RESPIRE branding logos.
- Dr Dominique Balharry, Morag Edwards, Dr Ai Keow Lim and Dr Chun Lin for their technical assistance and advice.
- Laura Merson and Nina Jamieson to share their wider global perspective.
- The RESPIRE Core team (Dr Genevieve Fernandes, Jay Evans, Dr Jayakayatri Jeevajothe Nathan, Laura Gonzalez Rienda, Laura Evans, Dr Siti Nur Husna Binti Muhamad, Dr Emma Kinley).
- The RESPIRE Unit Management Committee (UMC) for their patience and encouragement.

This work would not have been possible without the support and contributions of these individuals and organisations. Thank you all for your dedication and assistance.

Table of Contents

Summary	1
1.0 Introduction and Background	2
1.1 Introduction	2
1.2 Background	2
1.3 Purpose and benefits	2
1.3.1 Increased Visibility:	3
1.3.2 Enhanced Transparency	3
1.3.3 Greater Impact	3
1.3.4 Potential for Collaboration and Inclusive Knowledge	3
1.3.5 Increased Research Efficiencies	3
1.3.6 Reproducible Science	3
1.3.7 Balancing Openness with Data Protection and Ethics	3
1.4 Overview of Open Science	3
1.5 The need for a policy document	4
2.0 Ethical and Legal Frameworks	5
2.1 How can this policy document help each RESPIRE research project	5
2.2 Overview of Different Data Protection Provisions	5
2.2.1 Bangladesh	5
2.2.2 Bhutan	6
2.2.3 India	7
2.2.4 Indonesia	8
2.2.5 Malaysia	8
2.2.6 Pakistan	9
2.2.7 Sri Lanka	10
2.3 Overview of the General Data Protection Regulation (GDPR) and the UK Data Protection Bill 2018	10
3.0 Scope	11
3.1 Types of data that can be shared	11
3.2 Sensitive data to be preserved in a secure and responsible manner	11
4.0 Principles of Open Data Sharing	11
4.1 FAIR principles	12
4.1.1 Data Management Plans (DMPs)	12

4.1.2 Standardised Data.....	12
4.1.3 Open Licenses.....	13
4.1.4 Metadata and Documentation.....	13
4.1.5 Quality Assurance.....	14
4.1.6 Data privacy and protection while sharing sensitive data.....	14
5.0 Roles and Responsibilities	15
5.1 RESPIRE Supporting Platform III.....	15
5.2 RESPIRE Partners.....	16
5.3 Global Partners of RESPIRE Project	16
5.4 Principal Investigators (PIs), Co-Investigators (CoI) and Researchers	16
5.5 Within the University of Edinburgh and different RESPIRE Platforms	16
6.0 Data Sharing	17
6.1 How research data will be shared.....	17
6.2 Access Controls.....	19
7.0 Monitoring policy compliance & and Validity of the Policy Sharing.....	19
7.1 Data Monitoring Committee (DMC)	19
7.2 Periodic reviews & amendments	19
7.3 Periodic reviews & amendments	19
8.0 Training & Resources	20
8.1 Training Workshops by RESPIRE Platform III	20
8.2 Awareness workshops by the RESPIRE Partners.....	20
8.3 Mandatory Training in Data Protection	20
8.4 MANTRA	20
8.5 Additions and Alterations to the existing e-learning page of the RESPIRE Platform III Webnode.....	20
8.6 Curated Training Module for RESPIRE 2 Projects.....	20
8.7 Developing a Frequently Asked Questions (FAQ) along with Infographics Illustrations for Clarifying Common Misconceptions.....	20
9.0 Annexures.....	21
10.0 Contact	21
11.0 References.....	21
13.0 Appendix I: Data Protection and Relevant Legislation	23
14.0 Appendix II: University of Edinburgh Policies and Resources	25

Summary

This Open Data policy aims to:

- Promote FAIR (Findable, Accessible, Interoperable, and Reusable) data and Open Science in respiratory health research in Low- and Middle-Income Countries (LMICs).
- Ensure adherence to the legal and ethical frameworks governing data sharing in the RESPIRE Partner Countries: Bangladesh, Bhutan, India, Malaysia, Pakistan & Sri Lanka.
- Ensure compliance with Partner countries' data protection laws and regulations and the European Union's General Data Protection Regulation (GDPR).
- Ensure that informed consent is obtained from data subjects, that their rights and preferences are respected, ensure data security and confidentiality, and to minimise the risks of re-identification or misuse of data.
- Encourage the use of data repositories, metadata standards, data management plans, and licenses (CC BY) to facilitate data discovery, access, and reuse by other researchers and stakeholders.

Importance of data sharing vis-à-vis keeping privacy and security intact, along with ensuring the ethical considerations:

- Data sharing is essential for advancing scientific knowledge, fostering collaboration, enhancing transparency, and increasing the impact and value of research.
- Data sharing also benefits the health and well-being of the communities involved in the research, especially in LMICs, where respiratory diseases are prevalent, and resources are limited.
- In order to maintain the privacy and security of the participants, data sharing must be conducted responsibly and respectfully by adhering to ethical principles.
- Data sharing must comply with all relevant legal and regulatory frameworks that protect the rights and interests of participants and researchers.

Links to all references, guidance, and other resources cited in this document can be found in the reference list and appendices.

1.0 Introduction and Background

1.1 Introduction

The era of rapid technological advancements (comprising computing, cloud storage resources, smart handheld devices, and social media), has paved a new way to create and share academic research, thereby transforming the practice of science, which is now more open, more global and collaborative, and closer to society than ever.

Therefore, Open Science has become an increasingly important issue for funders and research institutions. It has quickly become crucial to all researchers because this widespread interest has emerged relatively recently; its definition and implementation are constantly shifting and evolving, sometimes leaving researchers in doubt about how to adopt Open Science and which are the best practices to follow (see Masuzzo and Martens, 2017).

1.2 Background

The University of Edinburgh is committed to fostering a culture of openness and collegiality among its researchers and their collaborators globally. As part of this commitment, the RESPIRE 2 Project (**NIHR Global Health Research Unit on Respiratory Health**), led by the University of Edinburgh and the Universiti Malaya, aims to deliver low-cost, scalable policy and clinical interventions to reduce respiratory disease and death in Asia. It has developed comprehensive policy guidelines to support Open Science and Open Data practices in the RESPIRE Project Partner Countries. In addition to providing a framework for ensuring Open Science practices across the project as a whole, this also helps the projects keep the momentum at par with the global drive for research excellence, Open Science, and data sharing.

1.3 Purpose and benefits

The purpose of this policy is to foster data sharing within the RESPIRE Projects in harmony with the principles of Open Science. In line with the requirements set forth by the project funders, this guidance aims to facilitate the sharing of research data as widely as possible and to promote a research environment that encourages transparency and collaboration. The ultimate goal is to advance knowledge and scientific progress while complying with legal and ethical requirements.

However, this guidance is not directed solely at RESPIRE research partners. It is also meant for all those associated with or engaging with stakeholders and researchers of the RESPIRE Project (see Staunton, et al., 2021).

The policy underscores numerous benefits arising from the adoption of open data-sharing practices within the RESPIRE Project LMICs. By making research data FAIR and accessible, the university and its Partners gain a number of advantages, such as:

1.3.1 Increased Visibility:

Allows research to transcend institutional and disciplinary boundaries. Findings reach a wider audience that includes fellow researchers, policymakers, and the public. By increasing visibility, a researcher's outputs gain recognition and may lead to new collaboration opportunities.

1.3.2 Enhanced Transparency

Fosters a transparent research environment, building trust among peers, policy makers, and the public, thereby reinforcing the credibility of research outcomes.

1.3.3 Greater Impact

Can result in increased citations and citations over longer periods of time for linked publications (Colavizza, 2020; Digital Curation Centre, 2017).

1.3.4 Potential for Collaboration and Inclusive Knowledge

Supports cross-institutional and international collaboration, fostering a culture of cooperation and shared knowledge. It also supports equal access to knowledge for researchers from diverse backgrounds and regions.

1.3.5 Increased Research Efficiencies

Reduces the duplication of effort and allows researchers to build upon existing datasets, saving time and resources, thus enhancing the overall productivity of the RESPIRE Project researchers. Similarly, researchers from other institutions and other projects can build upon the findings of RESPIRE partners, leading to new discoveries and innovations.

1.3.6 Reproducible Science

Enables other researchers to reproduce and validate the research findings to make them more robust.

1.3.7 Balancing Openness with Data Protection and Ethics

While advocating for data sharing, it also emphasises a balance between openness and protecting private and sensitive data as required by legal and ethical considerations.

1.4 Overview of Open Science

UNESCO has played a leading role in promoting Open Science. The 40th general conference, included discussions on globally agreed norms and efforts to create a standard-setting instrument. In 2021, the organisation adopted the Recommendation on Open Science, which provides a set of principles and guidelines for implementing Open Science. The Recommendation recognises the importance of open data as a key component of Open Science.

Open science is a movement to make scientific research and data more accessible, transparent, and collaborative. It is a broad concept that encapsulates the key practices: Open Access, Open Data, Open-Source Software, Open Peer Review, Citizen Science and Collaborative Research.

Open Data is a key component of Open Science. It refers to freely available data without restrictions (UNESCO, 2022).

As noted, there are many benefits to Open Science. It can help to accelerate scientific discovery, improve the quality of research, and increase public trust in science. It can also help bridge the digital divide between developed countries and LMICs to make scientific knowledge accessible to everyone.

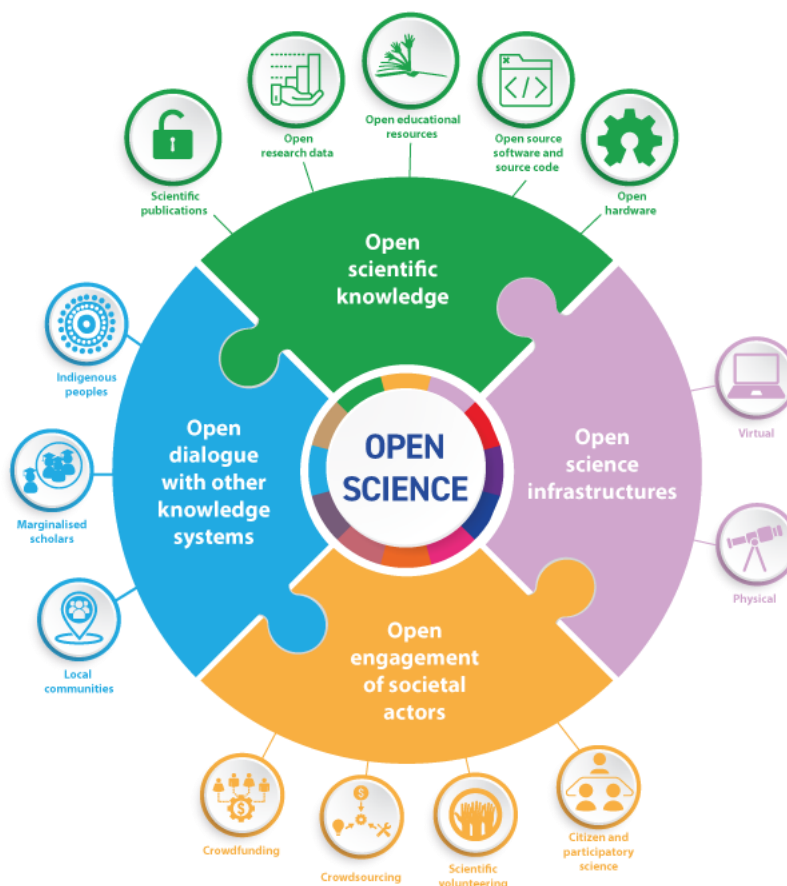


Figure 1 This image by author: [UNESCO](#) [7619] is licensed under [CC BY-SA 3.0 IGO](#) [12996]

1.5 The need for a policy document

In line with the commitment to openness as a fundamental value, the University of Edinburgh acknowledges the significance of promoting this principle throughout the RESPIRE project. This project extends to both the United Kingdom and several LMICs: namely, Bangladesh, Bhutan, India, Indonesia, Malaysia, Pakistan, and Sri Lanka. It promotes open access to publications and data with the aim of benefiting a wider readership. At the same time, however, it also safeguards the privacy and security of the individuals participating in research studies which come under the RESPIRE umbrella.

In this context, it becomes imperative to establish a comprehensive policy document that both expresses this commitment to Open Science while recognising legal and ethical requirements relating to personal and sensitive data (Angelaki, 2021).

2.0 Ethical and Legal Frameworks

2.1 How can this policy document help each RESPIRE research project

Research integrity and transparency are foundational for Research Data Management. An awareness of the various Data Protection laws that apply to the RESPIRE 2 partners is, therefore, essential. These laws make clear what we are *permitted* to do and what we *must* do when working with participant data.

In particular, all partners *must* ensure that their project teams are aware of their responsibilities under local and UK Data Protection laws. Furthermore, all partners and their project teams *must* ensure that data collection, storage, and sharing activities comply with those laws.

To facilitate this, Participant Information Sheets should clearly explain the plans for data sharing and archiving that have been adopted by RESPIRE 2 and its partners.

2.2 Overview of Different Data Protection Provisions

The following are summaries of Data Protection legislation in Bangladesh, Bhutan, India, Indonesia, Malaysia, Pakistan, Sri Lanka, and the UK. For a complete list of data protection legislation and links (where available at the time of writing), see Appendix I below.

2.2.1 Bangladesh

Provisions for data protection and privacy are enacted under

- The Constitution of the People's Republic of Bangladesh (point 43)
- The Information Communication Technology Act 2006 (point 63)
- The Right to Information Act 2009
- The Digital Security Act 2018

Under the Digital Security Act, the National Digital Security Council has the authority to formulate and issue data protection guidance. The Digital Security Agency has executive power over matters such as blocking content or decrypting a data source.

The Digital Security Act 2018

- Aims to ensure digital security and the identification, prevention, suppression, and trial of offenses committed through digital devices (Chapter I, Preliminary).
- Establishes the Digital Security Agency to oversee digital security matters (Chapter II, Digital Security Agency).
- Provides the power to remove or block data-information that threatens digital security (Chapter III, Preventive Measures).
- Defines and protects the critical information infrastructure against digital threats (Chapter V, Critical Information Infrastructure).

Right to Information Act 2009

The Right to Information Act makes provision for the free flow of and guarantees the peoples' right to information. In so doing, it ensures the transparency and accountability of all public, autonomous and statutory organisations and of all private organisations funded by the government of Bangladesh (Sections 2, 5, 8).

As part of Digital Bangladesh, the Open Government Data Strategy covers data generated by a number of different sectors. These include health, education, agriculture, tourism, finance and banking.

The Strategy defines the Scope of Data Sharing as

- Maximising use: Ready access to government-owned data will enable more extensive use of a valuable public resource for the benefit of the community
- Avoiding duplication: By sharing data, the need for separate bodies to collect the same data will be avoided, resulting in significant cost savings in data collection
- Maximised integration: By adopting common standards for the collection and transfer of data, integration of individual data sets may be feasible.
- Ownership information: The identification of owners for the principal data sets provides information on prioritised data collection programs and the development of data standards.
- Better decision-making: Data and information facilitate making important decisions without incurring repetitive costs.

2.2.2 Bhutan

The Information, Communications, and Media Act 2018 is the primary legislation governing the ICT and media sector in Bhutan. The Act contains provisions for the protection of data and privacy as well as data subject rights.

Principles of the Act are

- Lawfulness, fairness, and transparency: The collection, collation or processing of personal data must be lawful, fair, and transparent. Individuals must be informed about how their data is being collected and have the right to access and correct their data (Chapter 21, Points 384-385, p. 119).
- Purpose limitation: Personal data may only be collected and processed for specific purposes, and may not be used for any other purposes without the consent of the person concerned (Chapter 22, Point 388, p. 120).
- Data minimisation: The information collected shall be stored and used for the intended purpose only and may be removed or withdrawn upon the request of the users (Chapter 17, Point 340, p. 105).
- Accuracy: Personal data must be accurate and retained in the format in which it was generated (Chapter 14, Point 282, p. 84).
- Storage limitation: Personal data, including sensitive personal data or information, which are no longer necessary, shall be deleted (Chapter 21, Point 386, p. 119).
- Cyber Security: All personal data shall be protected from unauthorised access, use, disclosure, alteration, or destruction (Chapter 20, Point 375, p. 116).
- Accountability: Data controllers must demonstrate compliance with the Act's data protection and privacy requirements (Chapter 22, Point 387, p. 120).

The Act also established the Bhutan InfoComm and Media Authority (BICMA), making it responsible for enforcing the Act's data protection and privacy provisions. BICMA is an autonomous authority with the powers such as the ability to investigate complaints, issue orders, and impose fines (Chapter 3, Points 28-32, p. 9).

Nota bene, the Act applies to any offence committed outside Bhutan if the offence involves a computer system or network located in Bhutan (Chapter 1, Point 4, p. 2).

2.2.3 India

The Digital Personal Data Protection Act (DPDP Act, 2023) and the Information Technology Act (IT Act, 2000) are the two laws governing the privacy and protection of personal data in India.

The DPDP Act regulates the collection, processing, and use of personal data by government agencies and private companies in India. It prescribes the principles to be followed by any organisation collecting, processing, or storing personal data. It ensures that individuals have control over their personal data and that their data is used responsibly and ethically.

The principles

- Lawfulness, fairness, and transparency: Organisations may collect, process, and store personal data for lawful purposes only, and they must be transparent about how they are using the data (Chapter II, Section 4, p.4).
- Purpose limitation: Organisations must only collect personal data necessary for the purposes for which it is being collected and not be used for any other purpose without the data subject's consent (Chapter II, Sections 4,7, p.4,6).
- Accuracy: Organisations must take reasonable steps to ensure that the personal data they collect is accurate and up-to-date (Chapter II, Section 8(3), p.7).
- Storage limitation: Organisations must store personal data for as long as it is necessary for the purposes it is being collected (Chapter II, Sections 8(7), p.7,8).
- Security: Organisations must take reasonable steps to protect personal data from unauthorised access, use, disclosure, alteration, or destruction (Chapter II, Section 8(5), p.7).
- Accountability: Organisations must be accountable for the personal data they collect, process, and store (Chapter II, Section 8, p.7).

In addition to these general principles, the Act also has specific provisions that apply to processing personal data outside India's territory if such processing is in connection with any activity within the territory of India (Chapter I, Section 4(2), p.5).

- Application of Act: The Act applies to the processing of digital personal data outside the territory of India if the processing is related to offering goods or services to Data Principals within India.
- Transfer Restrictions: The Central Government may restrict the transfer of personal data by a Data Fiduciary for processing to certain notified countries or territories outside India.
- Exemptions: Certain exemptions exist where the Act's provisions do not apply, such as when processing is necessary for enforcing legal rights or claims or for processing by courts or tribunals in India for their judicial functions.

These provisions ensure that the personal data of individuals within India is protected even when processed outside the country, subject to the conditions of the Act.

The Data Protection Board of India will be formed to adjudicate non-compliance with the provisions of the Act.

The IT Act provides legal recognition for transactions carried out using electronic communication (electronic commerce), which involves electronic communication and storage of information. It also has a confidentiality and privacy clause, requiring that information must not be disclosed/shared without the consent of the data subject.

2.2.4 Indonesia

The Personal Data Protection Law of Indonesia (PDPL, 2022) regulates personal data processing in Indonesia. The PDPL applies to all organisations that process personal data (both electronic and non-electronic means) in Indonesia, regardless of their size or location. It establishes the Indonesian Data Protection Authority (DPA) and its roles and responsibilities.

The PDPA principles

- **Lawfulness:** Personal data must be processed lawfully, fairly, and transparently with the data subject.
- **Purpose limitation:** Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- **Data minimisation:** Personal data must be adequate, relevant, and limited to what is necessary for the purposes for which they are processed.
- **Accuracy:** Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal inaccurate data, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **Storage limitation:** Personal data must be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- **Integrity and confidentiality:** Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.

Furthermore, the PDPA provides for various rights for data subjects, including the rights to:

- Access their personal data
- Request that their personal data be corrected or deleted
- Object to the processing of their personal data
- Data portability

The PDPA also includes provisions for data transfer or transmission outside of Indonesia, such as Organisations must ensure that the recipient of the personal data provides adequate protection through a data transfer agreement with the recipient of the personal data.

2.2.5 Malaysia

The Personal Data Protection Act (PDPA, 2010) of Malaysia established the Personal Data Protection Commission (PDPC) to oversee compliance.

Data Protection principles

- **General Principle:** Personal data must be processed fairly and lawfully (Section 6, p.19).
- **Notice and Choice Principle:** Individuals must be notified of the purpose for which their personal data is being collected and informed consent to be taken in writing that their personal data is being processed (Section 7, p.20).
- **Disclosure Principle:** Personal data must not be disclosed to third parties without the individual's consent (Section 8, p.21).



- Security Principle: Personal data must be kept secure and protected against unauthorized access, disclosure, or misuse (Section 9, p.22).
- Retention Principle: Personal data must not be kept longer than necessary for the purpose for which it was collected (Section 10, p.23).
- Data Integrity Principle: Personal data must be accurate, complete, and up-to-date (Section 11, p.23).
- Access Principle: Individuals have the right to access their personal data and request correction if it is inaccurate (Section 12, p.23).

There are a few restrictions and procedures for compliance with the PDPA, in Malaysia.

- The PDPA does not expressly prohibit the storage of personal data outside of Malaysia. However, as a general principle, the identities of study participants will be protected and not shared.
- Only anonymised data will be shared publicly to protect personal data. The degree to which data is anonymised must be clearly understood and documented (Sections 6-12).

The Act allows law enforcement and regulatory authorities to access personal data under certain conditions, such as compliance with legal obligations or for the administration of justice (Section 6(2)).

Organizations failing to comply with the Act's provisions may face penalties, including fines and imprisonment, depending on the nature of the offense (Section 5(2)).

2.2.6 Pakistan

The Constitution of the Islamic Republic of Pakistan guarantees the privacy of Pakistani citizens as a fundamental right.

Personal Data Protection Bill (PDP, 2021) provides individuals with control over their personal data. The same provision only allows personal data to be transferred outside of Pakistan when the country to which data will be transferred offers at least the same level of personal data protection. The Pakistan Data Protection Authority (PDPA) will be established by the Bill to oversee compliance.

The PDPA is based on the following principles

- Lawfulness, fairness, and transparency in the collection, processing, and use of personal data (Chapter II, p.8).
- Purpose limitation: Personal data must only be collected for specific purposes and not be used for any other purpose without the individual's consent (Chapter II, p.8).
- Data minimisation: Only the minimum amount of personal data necessary for the purpose it is being collected should be collected (Chapter II, p.8).
- Accuracy: Personal data must be accurate and up-to-date (Chapter II, p.10).
- Storage limitation: Personal data must be stored for as long as necessary for the purpose it is being collected (Chapters II-III, p.10,19).
- Security: Appropriate measures must be taken to ensure the personal data's security from unauthorised access, use, disclosure, alteration, or destruction (Chapter II, p.9).
- Accountability: Organizations must be accountable for the personal data they collect, process, and store (Chapter II, p.8).

2.2.7 Sri Lanka

The Personal Data Protection Act, No. 9 (PDPA, 2022) identifies and strengthens the rights of data subjects in relation to the protection of their personal data and provides for the establishment of the Data Protection Authority (DPA) (PDPA, 2022, p.1).

The principles of the PDPA are as follows

- Lawfulness, fairness, and transparency: The processing of personal data shall be lawful, fair, and transparent (Section 5, p.4).
- Purpose limitation: To ensure that personal data is processed for a specified, explicit, and legitimate purpose, and such personal data shall not be further processed in a manner incompatible with such purposes (Section 6(1), p.4).
- Data minimisation: To ensure that personal data that is processed shall be adequate, relevant, and proportionate to the extent as is necessary in relation to the purpose for which such data shall be collected or processed (Section 7, p.5).
- Accuracy: Ensuring the processed personal data shall be accurate and kept up to date (Section 8(a), p.5).
- Storage limitation: To ensure that personal data that is being processed shall be kept in a form which permits identification of data subjects only for such period as may be necessary or required for the purposes for which such personal data is processed (Section 9, p.5).
- Security: Every controller shall ensure the integrity and confidentiality of personal data being processed by using appropriate technical and organisational measures, such as encryption, anonymisation, access controls etc. (Section 10, p.5-6).
- Accountability: Every controller shall implement internal controls and procedures (Data Protection Management Programme) that establish and maintains duly catalogued records to demonstrate how the implementation of the data protection obligations is carried out by the controller (Section 12(1)(a), p.7).

The Act also addresses cross-border data flow and the protection of personal data outside Sri Lanka (Section 26).

2.3 Overview of the General Data Protection Regulation (GDPR) and the UK Data Protection Bill 2018

The UK General Data Protection Regulation (GDPR, 2018) covers the processing of all Personal and Special Category data. Processing includes any and all operations performed upon the data, from collection to disposal.

- Personal data is data that relates to an identified or identifiable individual person.
- Special Category data relates to the race, ethnic origin, politics, religion, genetics, sex life, or health of an identified or identifiable individual person.
- UK GDPR applies to anyone in the UK/EU who processes personal data anywhere in the world and anyone outside the UK/EU who processes personal data on UK/EU citizens.

This means that:

- a) Data collected by UK-based researchers from participants anywhere in the world is protected by UK GDPR;
- b) Data collected by researchers anywhere in the world from UK-based participants is also protected by UK GDPR.

UK GDPR consists of the following seven principles

- Data must be processed lawfully, fairly and transparently.
- The purposes for which data is collected must be specified, explicit, and legitimate; researchers must keep to the original specified purposes and not further process data in a manner that is incompatible with them.
- Data must be relevant and limited to what is necessary to fulfil the purposes for which the data is collected.
- Data must be accurate and, where necessary, kept up to date.
- Data should not be retained for longer than is necessary for the fulfilment of the specified purposes for which it was collected.
- Appropriate technical and organisational measures must be applied to prevent unauthorised or unlawful access, loss, or destruction, or damage to data.
- The researcher is accountable for ensuring compliance of all data processes with GDPR.

Since legislation is dynamic by nature, please contact your Local Data Protection Authority and/ or the ethics committee of your institution for advice on how to safeguard the personal data of participants in your study.

3.0 Scope

3.1 Types of data that can be shared

Data that has been anonymised and contains no personally identifiable information will be deposited in an Open Access repository such as [Edinburgh DataShare](#).

The optimum time for making data available in an Open Access repository is at the same time as the findings are published. Data that has been deposited in DataShare can be embargoed for up to two years before it is made openly available.

3.2 Sensitive data to be preserved in a secure and responsible manner

Data which cannot be made openly accessible because it contains personally identifiable information must still be preserved for the purposes of verification and replication of research findings. Such data should be deposited in a restricted access repository, such as [Edinburgh DataVault](#).

Please note, active data storage, e.g., institutional network and cloud-based solutions, are not appropriate for long-term preservation or archiving. Data that is left on active storage long-term gets forgotten about and lost, thereby undermining the research to which it pertains. Therefore, all research data must be deposited in a suitable repository.

4.0 Principles of Open Data Sharing

There is a broad, global consensus that publicly funded research projects such as RESPIRE 2 should make their research data as accessible as legal and ethical commitments permit. For this reason, the University of Edinburgh has embraced FAIR principles for research data. (Details of this and other key commitments can be found in the [University of Edinburgh Research Data Management Policy](#)).

FAIR principles allow researchers to plan for open data sharing while acknowledging legitimate reasons for restricting access to data, such as confidentiality. Following the [European Research Executive Agency and the Horizon programme](#), our maxim is, therefore:

4.1 FAIR principles

Details of the **FAIR principles** as well as guidance on how to implement them can be found on the [GOFAIR website](#).



In brief, however, making research data **FAIR** means ensuring that research data is:

Findable	Accessible	Interoperable	Reusable
archived in a repository, has good metadata, assigned a persistent identifier (e.g. a DOI)	access conditions/restrictions are clear	uses open/standard file formats, metadata is machine-readable	has good documentation and metadata, is licensed (CC BY 4.0), is citable

Partners and their project teams should ensure that Data Management Plans reflect the RESPIRE project's commitment to FAIR Principles **by providing information** on how the above requirements will be met.

4.1.1 Data Management Plans (DMPs)

DMPs should be created to outline how data will be collected, managed, and shared (Annexure: University of Edinburgh's DMP templates; RESPIRE DMP template and guidance)].

4.1.2 Standardised Data

The format for text and data tables must be standardised to ensure consistency and Interoperability across different systems/ platforms.

Implementing FAIR Data principles requires that all data management activities from collection to preservation be standardised. This will help ensure that all the datasets collected by the different partners are well-organised and documented and therefore:

- a) easy to Find and Access; and
- b) securely stored.

Standardising the layout and file format of data files will facilitate Interoperability with other datasets, workflows, and platforms.

Standard practices, layouts, formats, etc. should all be clearly detailed in the project's Data Management Plan.

4.1.3 Open Licenses

FAIR data should be licenced. Without a licence it can be extremely difficult, if not impossible, for other researchers to make use of the data. It is recommended that a Creative Commons Attribution licence (CC BY) be applied to data when it is deposited in a repository. A CC BY licence means the data is open and accessible on condition that the data owner is properly cited.

4.1.4 Metadata and Documentation

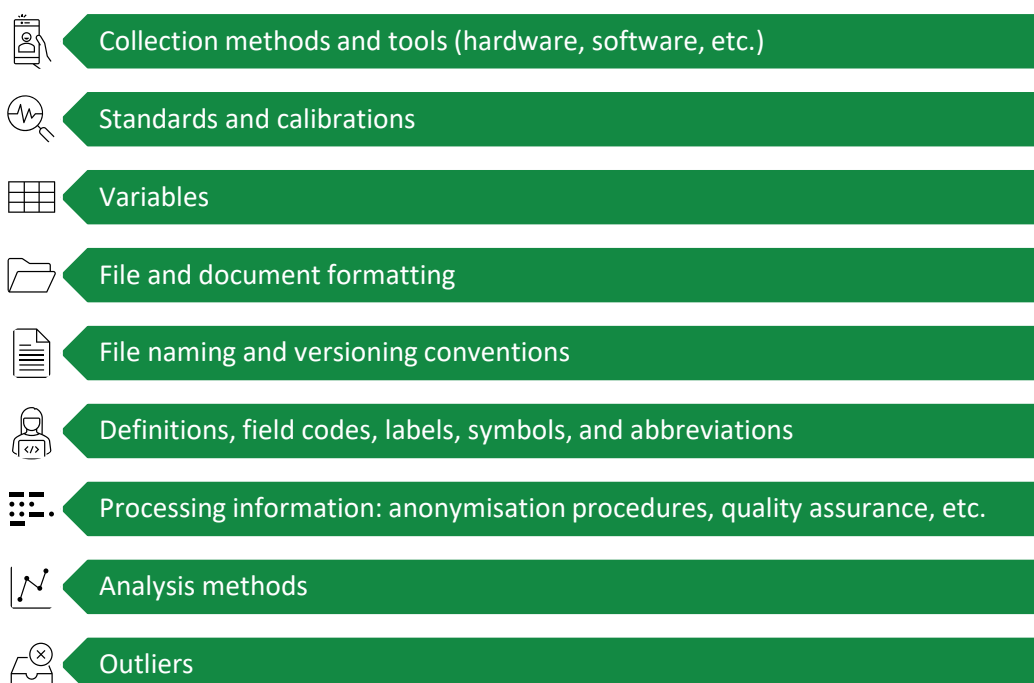
FAIR data requires good metadata. Metadata provides valuable contextual information about the data, including:

- Dataset Title
- Data Creator
- Data type
- Date
- Location of data creation
- File Formats

Good metadata should provide enough information to make recreating the dataset it relates to relatively simple.

All partners should **use the metadata template provided** (Annexure: RESPIRE Metadata template). This will ensure that metadata is standardised and that, as a consequence, datasets created by different partners are fully interoperable.

In addition to standard metadata, it is recommended that **ReadMe documentation** is created for all datasets. A ReadMe document is a plain text file stored alongside the dataset. It contains details on how to identify, access, interpret, and analyse the dataset to which it refers. Standard ReadMe documentation may include:



To make data as FAIR as possible, it is recommended that ReadMe Documentation is standardised across projects.

4.1.5 Quality Assurance

Partners **must implement quality assurance processes to ensure the accuracy and consistency of research data**. These processes should be documented in the project DMP. They should include Standard Operating Procedures and Protocols with built-in quality checks for all data processing activities: collection, data entry, transcription, anonymisation, and analysis. Quality assurance processes do not need to be complicated or excessively formal; for example, they may include activities such as colleagues proofreading or reviewing data.

It is very important, however, that data is properly organised, documented, and labelled. File naming conventions must be consistently applied to clearly distinguish between raw, processed, and final data.

4.1.6 Data privacy and protection while sharing sensitive data

When working with personal and sensitive data – e.g. health data – it is extremely important to ensure that the proper safeguards are in place. Preventing unauthorised access to personal/sensitive data requires a DMP that details how the data is being collected and how it will be managed during the lifetime of the project.

In addition to a clearly documented and consistently applied approach to data organisation, documentation, naming and version conventions, other standard safeguards include:

Secure storage:

- Always use an institutionally owned/managed network or cloud-based storage.
- Do not use portable storage devices such as USB sticks or external hard drives unless absolutely necessary; if portable devices are used, back up to secure storage as soon as possible.
- Do not store data on laptop or desktop hard drives.

Encryption:

- Keep personal/sensitive data in an encrypted container.
- Keep contact details, pseudonymisation keys, etc. in separate encrypted containers.
- When working in the field always ensure that laptops and other devices are encrypted.

De-identification:

- De-identify personal/sensitive data at the earliest possible opportunity.

Controlled access:

- Ensure that only those members of the project team who need access to personal/sensitive data have access to personal/sensitive data.

Training:

- Ensure that every member of the project team has completed data protection training and is aware of their responsibilities.

5.0 Roles and Responsibilities

There are a number of different roles and responsibilities within RESPIRE Programs and platforms and within different Partner sites.

5.1 RESPIRE Supporting Platform III

Supporting Open Access/Open Science:

- Provide training and awareness workshops and provisioning of infrastructure.

Delivering additional training in collaboration with Platform II:

- In coordination with Platform II, provides supplementary training to project staff. The training focuses on data management, Open Science principles, and relevant skills to ensure effective implementation of open data practices.

Storing research data:

- Facilitating access and supporting researchers with guidance for depositing and sharing research data in the University of Edinburgh's DataShare service.

Depositing all data in local repositories with anonymised data stored with the University of Edinburgh:

- Ensuring all project data is deposited in designated local repositories maintaining a register with links. Additionally, anonymised data is deposited with the University of Edinburgh to protect the participants' privacy.

Monitoring policy compliance:

- Conduct regular Data Monitoring Committee meetings to review trial data, assess safety concerns, and make informed decisions to guide the sites in line with the GDPR, local data protection acts and regulatory rules, based on the data collected during the RESPIRE trials.
- Mandating the use of Digital Object Identifiers (DOI) generated from University of Edinburgh's DataShare for in all publications along with Data Access Statements in all publications.
- Appointing/ designating a Data Officer responsible for all matters relating to data. The Data Officer will ensure the creation of DMPs, compliance with respective LMICs' and GDPR legislations, and oversight of data curation and stewardship activities.

Open Licensing policy:

- Have a policy that recommends CC BY and provides guidance on other licenses when appropriate. For information on Open Licences, see [Open.Ed, Open Educational Resources, 'Understanding open licences.'](#)

Policy guideline:

- Have a Policy guideline in place to support Open Science.

Transferring all the anonymised study data in University of Edinburgh's DataShare:

- Platform III coordinates the transfer of all project data to the University of Edinburgh's DataVault for the preservation and availability of data for future research and analysis.



5.2 RESPIRE Partners

Managing publications, data and educational resources in adherence with the principles and requirements expressed in this Policy.

Registering new research projects' appropriate service (e.g. Pure, which is the University's Current Research Information System). Information held in Pure relates to research staff and their publications to ensure they receive the appropriate institutional support.

Complying with the organisational, regulatory, institutional, and other contractual and legal requirements related to the production, curation, deposit, management, and distribution of publications and data in case there is no other agreement with third parties taking precedence.

5.3 Global Partners of RESPIRE Project

Reporting on the total cost of scholarly publication channels and individual publications and making these reports publicly available.

Engaging in discussions concerning agreements with publishers to include the right to publish all articles Open Access or make them openly and immediately available via a repository route at the time of publishing.

Supporting skills development for students and employees to foster Open Science.

5.4 Principal Investigators (PIs), Co-Investigators (CoI) and Researchers

Writing a DMP for every research project they are coordinating and ensuring the adherence thereto.

Ensuring DMPs comply with the policy guidance and NIHR data management and sharing requirements.

Assigning a CC BY license to their research outputs and ensuring that research data is made open in a timely manner.

5.5 Within the University of Edinburgh and different RESPIRE Platforms

The four supporting platforms of the RESPIRE Project aligned with the Guidelines, these platforms create a collaborative and inclusive research environment and work together to foster Open Science.

The project creates a collaborative and inclusive research environment by engaging stakeholders, building research capacity, embracing Open Science principles, and leveraging digital health solutions.

This environment promotes transparency, reproducibility, and the responsible use of data, ultimately advancing respiratory health research and improving outcomes for the communities involved.

6.0 Data Sharing

In accordance with University of Edinburgh Research Data Management Policy and RESPIRE Data Management guidance (see appendix 11.2), RESPIRE 2 has adopted a FAIR approach to data sharing. Minimally, all research partners are required to ensure that data collected or generated as part of RESPIRE 2 is made available for the purposes of verification, replication, and reuse.

Research partners are required to make their research data open at the earliest possible opportunity. In practice, this means whichever of the following comes first; either:

- At the same time that findings based up on the data are published;

or

- At the end of the project/funding period.

6.1 How research data will be shared

In order to ensure timely and effective data sharing, it is essential that PIs plan to share. A clear strategy for how, when, and where data will be made accessible must be part of the project's DMP. This strategy should be updated during the project lifetime, as and when circumstances affecting Data Sharing arise.

Where data collected from human participants – via surveys, interviews, etc. – is to be shared, participant consent should be sought. When consenting participants for data sharing, it is important to explain clearly that only anonymised data will be shared and that personally identifying information will continue to be safeguarded against unauthorised access.

Furthermore, to ensure that consent to share is informed consent: researchers should clearly explain what data sharing is and why it is being done. Adopting a simple communications strategy will make this process easier.

For example, a simple three-step Communications Strategy:

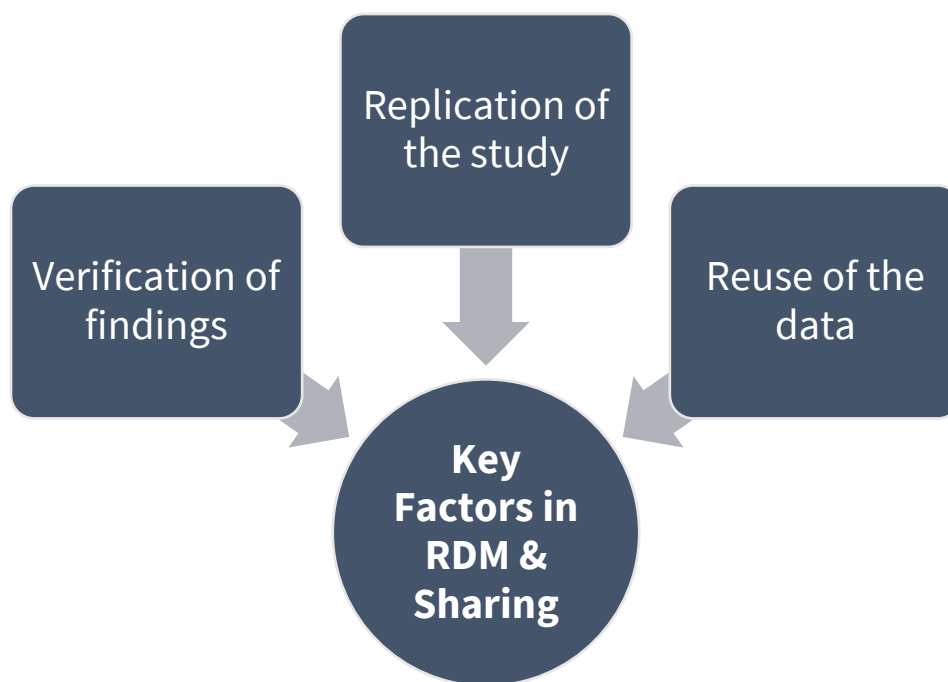
1. Define your terms	2. Give your reasons	3. Explain the benefits
• Data Sharing • Making data available to other researchers; • At institutions anywhere in the world; • In this and other fields of academic research; • Shared openly • Data Preservation • Long-term storage of the data in a suitable data repository	• Verification • Confirming the accuracy of research findings • Reproducibility • Confirming that repeating the study will achieve the same results • Reuse • Use of the data for purposes other than those for which it was originally collected • Use of the data for another, different research project	• Integrity • Proper ethical procedures and safeguards have been followed/applied • Verifiable research findings • Accuracy and rigour of Scientific Record • Transparency • Showing your working • Research design, methods, conduct, and outcomes can be checked • Progress • Reusing data saves time and speeds up medical research

As stated in the University of Edinburgh Research Data Management Policy, Research Data should be offered for deposit in a suitable national or international data service, disciplinary repository, or institutional repository.

The University of Edinburgh provides the free-at-point-of-use, open-access digital repository: Edinburgh DataShare. DataShare is a trusted digital repository with the [CoreTrustSeal](#). To promote data discovery, it is optimised for search engines and indexed in Google Scholar and Google Dataset.

For RESPIRE 2 research partners, the process of depositing data in DataShare is more complicated than it would be for University of Edinburgh staff. It is likely that this process will involve transferring the data to a member of the project team based in Edinburgh. That person will then deposit the data on behalf of the research partner. The deposit process will be supported by the University of Edinburgh Research Data Support team.

Additionally, as indicated, the principal drivers behind research data management and sharing activities are:



Given these drivers and the aforementioned complications, research partners must ensure that their research data is properly prepared for deposit.

Preparation for deposit:

- Double-check for personally identifiable information – DataShare is an Open Access repository, therefore only de-identified can be accepted;
- Data must be well-structured and organised;
- Data must be well-documented – minimally, all datasets must be accompanied by a ReadMe file; where possible, additional metadata and contextual information should also be included with the deposit;
- The deposit must include a clear description of the data.



All accepted deposits will be assigned a DOI. This is a permanent link to the data location and should be used in all publications, conference papers, and other communications (e.g. social media posts) which refer to the data. Accepted deposits will be assigned a CC BY 4.0 licence, which enables the re-use of the data on condition that the data creator is properly credited.

Accepted deposits will have a corresponding metadata record created in the University of Edinburgh's Pure system. This will facilitate discovery of the data. It is recommended that, where possible, research partners ensure that a metadata record is created for the data in their institutional research information systems; this should include the DOI to enable easy navigation to the data location.

Research data containing personally identifying information should still be archived for the purposes of verification and replication. In such cases, researchers should identify a suitable local alternative, such as institutional secure network storage, and keep the data encrypted at all times. Research data containing personally identifying information should still be well documented to make it findable, accessible, and interpretable. Minimally, these datasets should be accompanied by a ReadMe file – including details of de-identification processes – additional metadata, and contextual information.

6.2 Access Controls

Data deposited in Edinburgh DataShare is Open Data and therefore not subject to access controls. Governance of reuse is restricted to the licensing of the data.

When depositing data, researchers have the option to request a time-limited embargo that will ensure data is not made public before related publications. Once this embargo expires, all accepted submissions are archived and available indefinitely.

7.0 Monitoring policy compliance & and Validity of the Policy Sharing

7.1 Data Monitoring Committee (DMC)

A Data Monitoring Committee will be established to monitor compliance with this policy. Regular DMC meetings will be held to review trial data, assess safety concerns, and make informed decisions based on the data collected during the RESPIRE studies.

7.2 Periodic reviews & amendments

The document will be reviewed annually to ensure that it remains aligned with the policies and legislation referred to herein. It will also be reviewed by Platform III (University of Edinburgh) in consultation with RESPIRE partners and other stakeholders to ensure that data management guidance is kept up to date. Significant changes to policies, legislation, or RDM practice will be noted in the meantime, and the document amended accordingly.

7.3 Periodic reviews & amendments

Feedback from the RESPIRE Partners is essential to improve the policy and incorporate any changes arising from their experiences and challenges. The RESPIRE Partners are encouraged to share concerns relating to policy implementation, data management, data sharing, and any other issues or barriers they may face.

Please send feedback to Tapas.Mohanty@ed.ac.uk Cc tapasblog@gmail.com, RESPIRE@ed.ac.uk

8.0 Training & Resources

8.1 Training Workshops by RESPIRE Platform III

In cooperation with the University of Edinburgh's Research Data Support team, supporting Platforms (I, II, IV) and appropriate bodies (such as legal services, research support staff, and RDM experts), Platform III will provide Open Science training workshops and resources. These workshops will cover topics such as open-access publishing, FAIR and open data and data management, research integrity, and reproducibility.

8.2 Awareness workshops by the RESPIRE Partners

RESPIRE Partners are expected to provide training and awareness workshops on local Personal Data Privacy legislation to ensure that researchers and other staff are kept up-to-date.

8.3 Mandatory Training in Data Protection

University of Edinburgh's Data Protection Policy mandates requires that all researchers complete training in Data Protection and Data Protection for Research. Where the University's learning platform is not accessible, as with research partners, the Research Data Support team recommends that researchers complete the UK Medical Research Council training course, '[New Oct 2025: Confidentiality and Data Protection in Health Research](#)' (formerly known as Research, GDPR and Confidentiality – what you need to know).

The training can be accessed by signing up through:

<https://bygsystems.net/mrcrsc-lms/enrol/index.php?id=95>

8.4 MANTRA

MANTRA is a free, online non-assessed training suite, which will help you to understand and reflect upon how to manage the digital data you collect throughout your research study. Information is presented from a range of perspectives, including post-graduate students, early career researchers, PIs, and information professionals. It is freely available on the web for anyone to explore independently.

8.5 Additions and Alterations to the existing e-learning page of the RESPIRE Platform III Webnode

To strengthen the understanding of RESPIRE Partners on Open Science, Open Data, and Open Access Publishing, additional modules will be made based on the need assessment and requirements received from them. The resources will be made available and shared with the partners.

8.6 Curated Training Module for RESPIRE 2 Projects

To ensure a comprehensive approach to Open Science, a curated training module will be designed specifically to address the needs of RESPIRE 2 Projects and partners.

8.7 Developing a Frequently Asked Questions (FAQ) along with Infographics Illustrations for Clarifying Common Misconceptions

Since Open Science is a relatively recent development it is expected usual that there will be misconceptions. To address these and promote a clear understanding a Frequently Asked Question (FAQ) document plus infographics will be developed. These will be made available to RESPIRE Partner institutions, researchers, staff, as well as the wider public.

9.0 Annexures

The following templates are included at the end of this document:

- 9.1 RESPIRE Data Management Plan (DMP): Template (adapted from the University of Edinburgh)
- 9.2 RESPIRE Data Management Plan Guidance & Checklist
- 9.3 RESPIRE METADATA: Template
- 9.4 RESPIRE METADATA Schema
- 9.5 AUTHOR DATASET ReadmeTemplate
- 9.6 Standard Operating Procedure (SoP) Template

10.0 Contact

If you have any queries about the information contained in this document

For sharing feedback, general queries, and requests, please email Tapas Kumar Mohanty, Informatics and Data Science Liaison Officer at Tapas.Mohanty@ed.ac.uk or tapasblog@gmail.com with a CC RESPIRE@ed.ac.uk

11.0 References

Angelaki, M. (2021) *Model policy on open science for research performing organisations (RPOs)*. Zenodo. Available at: <https://doi.org/10.5281/zenodo.4666050>.

Carroll, S., Garba, I., Figueroa-Rodríguez, O. L., Holbrook, J., Lovett, R., Materechera, S., Parsons, M., Raseroka K., Rodriguez-Lonebear, D., Rowe R., Sara, R., Walker, J. D., Anderson J., and Hudson M. (2020) 'The CARE principles for Indigenous data governance', *Data Science Journal*, 19: XX. Available at: <https://doi.org/10.5334/dsj-2020-043>.

Colavizza, G., Hrynaszkiewicz, I., Staden, I., Whitaker, K., and McGillivray, B. (2020) 'The citation advantage of linking publications to research data', *PLOS ONE*, 15(4), e0230416. Available at: <https://doi.org/10.1371/journal.pone.0230416>.

Masuzzo, P. and Martens, L. (2017) 'Do you speak open science? Resources and tips to learn the language', *Peer J Preprints*, 5:e2689v1. Available at: <https://doi.org/10.7287/peerj.preprints.2689v1>.

Mohanty, T. K., Smith, S., Bhattacharjee, T., Weir, C. J., and Norrie, J.; RESPIRE Collaboration. (2025) 'Open science policy guidelines promoting open data sharing in low and middle-income countries for respiratory health research under NIHR Global RESPIRE project', *Journal of Global Health*. Available at: <https://doi.org/10.7189/jogh.15.03021>.

Staunton, C., Barragán, C.A., Canali, S. Ho, C., Leonelli, S., Mayernik, M., Prainsack, B., and Wonkham, A. (2021) 'Open science, data sharing and solidarity: who benefits?', *History and Philosophy of the Life Sciences*, 43, 115. Available at: <https://doi.org/10.1007/s40656-021-00468-6>.

Wiebe, A. and Dietrich, N. (eds.) (2017) *Open data protection study on legal barriers to open data sharing – data protection and PSI*. Universitätsverlag Göttingen. Available at: https://univerlag.uni-goettingen.de/bitstream/handle/3/isbn-978-3-86395-334-8/wiebe_data%20protection.pdf

12.0 Guidance

CARE Principles for Indigenous Data Governance. Global Indigenous Data Alliance. <https://www.gida-global.org/care>. Accessed: 19th August 2025.

European Research Executive Agency. 'H2020 Programme Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020.' https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf. Accessed: 19th August 2025.

European Research Executive Agency. 'Open science. Q&A on what you should comply with when applying for funding and implementing your project.' https://rea.ec.europa.eu/open-science_en. Accessed: 19th August 2025.

FAIR Principles. GO FAIR Initiative. <https://www.go-fair.org/fair-principles/>. Accessed 10th October 2025.

Max Planck Society. 'Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities.' 2003. <https://openaccess.mpg.de/Berlin-Declaration>. Accessed: 19th August 2025.

National Academies of Sciences, Engineering, and Medicine. 2018. Open Science by Design: Realizing a Vision for 21st Century Research. Washington, DC: The National Academies Press. <https://doi.org/10.17226/25116>. Accessed: 19th August 2025.

OpenScience.eu. 'Open Science best practice projects and tools to foster FAIR research outputs.' <https://openscience.eu/>. Accessed: 19th August 2025.

Digital Curation Centre. (2017) Briefing Paper: The Open Data Citation Advantage. SPARC Europe. <https://sparceurope.org/open-data-citation-advantage>. Accessed: 19th August 2025.

UNESCO. 'Recommendation on Science and Scientific Researchers.' UNESCO Digital Library, 2018. <https://unesdoc.unesco.org/ark:/48223/pf0000263618>. Accessed: 19th August 2025.

UNESCO. 'UNESCO open science tool kit: Understanding open science.' UNESCO Digital Library, 2022. <https://doi.org/10.54677/UTCD9302>. Accessed: 19th August 2025.

UNESCO. 'Open Access.' <https://en.unesco.org/open-access/what-open-access>. Accessed: 19th August 2025.

13.0 Appendix I: Data Protection and Relevant Legislation

Information on the data protection legislation of each country mentioned below can be found at <https://www.dlapiperdataprotection.com/>.

Bangladesh: Government of the People's Republic of Bangladesh.

- The Constitution of the People's Republic of Bangladesh. <https://faolex.fao.org/docs/pdf/bgd117108E.pdf>
- Information Communication Technology Act, 2006. <https://samsn.ifj.org/wp-content/uploads/2015/07/Bangladesh-ICT-Act-2006.pdf>
- Right to Information Act of Bangladesh, 2009. <https://mrdibd.org/wp-content/uploads/2021/04/RTI-Act-English-1.pdf>
- Sohini Paul. 2009. The Right to Information Act, 2009, Bangladesh, A Summary. The Human Rights Initiative. https://www.humanrightsinitiative.org/programs/ai/rti/international/laws_papers/bangladesh/bangladesh_rti_act_2009_summary.pdf
- Open Government Data Strategy, 2016. <https://objectstorage.ap-dcc-gazipur-1.oraclecloud15.com/n/axvjbnqprylg/b/V2Ministry/o/office-bbs/2024/12/c212037978d8497e8298da0c0cc93ef0.pdf>
- Digital Security Act, 2018. <https://www.icnl.org/wp-content/uploads/Digital-Security-Act-2018-English-version.pdf>.

NB since completing this document, the Digital Security Act has been superseded by the Cyber Security Ordinance 2025. For information on this, see:

- Bangladesh Government Press, Government of the People's Republic of Bangladesh, Extraordinary Gazette of May 2025. https://www.dpp.gov.bd/bgpress/index.php/document/get_extraordinary/57587
- Digital Policy Alert. *Bangladesh: Cyber Security Ordinance, 2025 (Ordinance No. 25 of 2025) enters into force.* <https://digitalpolicyalert.org/event/38587-cyber-security-ordinance-2025-ordinance-no-25-of-2025-enters-into-force>
- Roy, Prakash Chandra, The Cyber Security Ordinance 2025: An Unofficial English Translation (August 28, 2025). Available at SSRN: <https://ssrn.com/abstract=5424414> or <http://dx.doi.org/10.2139/ssrn.5424414>

Bhutan: Parliament of Bhutan.

- Information, Communications, and Media Act, 2018. https://www.bicma.gov.bt/data/publications/act/BICM_Act_2018_English.pdf.
- The Bhutan InfoComm and Media Authority (BICMA). <https://www.bicma.gov.bt/>.

India: Ministry of Law and Justice of India.

- The Digital Personal Data Protection Act, 2023. <https://cag.gov.in/uploads/media/IT-ACT-20210330163049.pdf>.
- Information Technology Act, 2000. <https://cag.gov.in/uploads/media/IT-ACT-20210330163049.pdf>.
- For information on the Data Protection Board of India, see <https://dpdpaedu.org/docs/Overview/The%20Data%20Protection%20Board%20of%20India/>

Indonesia: The Indonesian House of Representatives.

- The Data Protection Law of Indonesia, 2022. <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>. An English version is not currently available online; see the summary at DLA Piper Intelligence: <https://www.dlapiperdataprotection.com/?t=law&c=ID>.

Malaysia: Parliament of Malaysia.

- The Personal Data Protection Act, 2010. [https://mohre.um.edu.my/img/files/Personal%20Data%20Protection%20\(PDPA\)%20Act%202010.pdf](https://mohre.um.edu.my/img/files/Personal%20Data%20Protection%20(PDPA)%20Act%202010.pdf).
- Personal Data Protection Commission. <https://www.pdp.gov.my/ppdpv1/akta/akta-pdp-2010>.

Pakistan: Ministry of Information Technology & Telecommunication of Pakistan.

- The Constitution of the Islamic Republic of Pakistan. <https://pakistani.org/pakistan/constitution/#gsc.tab=0>
- The Personal Data Protection Bill, 2021. [https://moitt.gov.pk/SiteImage/Misc/files/25821%20DPA%20Bill%20Consultation%20Draft\(1\).pdf](https://moitt.gov.pk/SiteImage/Misc/files/25821%20DPA%20Bill%20Consultation%20Draft(1).pdf)

Sri Lanka: Parliament of the Democratic Socialist Republic of Sri Lanka.

- The Personal Data Protection Act, No. 9, 2022. <https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf>.

UK: The UK Parliament

- Data Protection Act, 2018. <https://www.legislation.gov.uk/ukpga/2018/12/contents?view=plain>; https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf.

EU: European Parliament

- General Data Protection Regulation. <https://www.legislation.gov.uk/eur/2016/679/contents?view=plain>.

14.0 Appendix II: University of Edinburgh Policies and Resources

Rice, Robin (2021). University of Edinburgh Research Data Management Policy. University of Edinburgh. <http://dx.doi.org/10.7488/era/1502>.

Tate, Dominic. (2022). University of Edinburgh Research Publications & Copyright Policy. University of Edinburgh. <https://information-services.ed.ac.uk/about/policies-and-regulations/research-publications>.

University of Edinburgh Open.Ed, Open Educational Resources. 'Understanding open licences.' <https://open.ed.ac.uk/how-to-guides/understanding-open-licences/>.

University of Edinburgh. (2024). Edinburgh Open Research Roadmap. University of Edinburgh. <https://library.ed.ac.uk/research-support/open-research/about>.

University of Edinburgh. (2025). University of Edinburgh Position Statement on Open Research. University of Edinburgh. <https://library.ed.ac.uk/sites/default/files/2025-05/UoE%20Position%20Statement%20on%20Open%20Research.pdf>.

University of Edinburgh Research Data Services: <https://library.ed.ac.uk/research-support/research-data-service>.

University of Edinburgh DataShare: <https://datashare.ed.ac.uk>.

University of Edinburgh DataVault: <https://datavault.ed.ac.uk>.

University of Edinburgh Research Data Service: Trustworthy Digital Repository. <https://library.ed.ac.uk/research-support/research-data-service/after/data-repository/trustworthy-digital-repository>.

University of Edinburgh Research Data Services: MANTRA Research Data Management Training: <https://mantra.ed.ac.uk/>.

University of Edinburgh Research Data Services; University of North Carolina: Research Data Management and Sharing MOOC (Coursera): <https://www.coursera.org/learn/data-management>.



Annexures



9.1 RESPIRE Data Management Plan (DMP): Template (adapted from the University of Edinburgh)

Data Management Plan (DMP) Template

Name:	
Project Title:	
Institute:	
Start Date:	
End Date:	
DMP version number and date:	
<u>Responsibilities & Resources (applicable across the sections below)</u>	
<i>Who will be involved in the data management of this research?</i>	
1. Data Capture	
<i>What data will be generated or reused in this research?</i>	
<i>How much data will be generated?</i>	

2. Data Management

How will the data be documented to ensure it can be understood?

All metadata should be standardised using the metadata schema supplied.

Consider preparing ReadMe documentation for each dataset. A ReadMe file is a simple text document (.txt) which sits alongside your data files and explains:

- What the data is;
- What the data covers;
- Where it the data can be found (file path);
- Licensing and access conditions (e.g. confidentiality requirements).

Imagine that you are preparing to publish your study findings. A reviewer asks to see your data to verify your findings. What information will that reviewer need to be able to:

- Find the data they need (folder location, file name);
- Open or access your data (format, software requirements, access conditions);
- Understand or interpret your data (field codes, abbreviations, symbols, variables);
- Analyse your data (code, methods, outliers, missing data)?

ReadMe documentation should be standardised using a template.

Where will the data be stored and backed up?

To prevent loss, unauthorised access, accidental deletion, etc., data should not be stored on desktop or laptop hard drives or portable media such as flash drives. Data should be stored on your institution's networked storage.

A logical filing system should be set up (e.g. nested folders) with all folders and files clearly labelled. A standardised and meaningful file naming convention should be established for all folders and data files to make particular data files easy to find.

A file naming convention should include:

- No Special Characters: “”£\$%!~&*^()+=[]{ }~@:;#,.<>
- Underscore Spaces: _ or %20 may replace the space
- Reverse Dates for sorting: YYYYMMDD
- Version Control: Date_FileName_v1, _v2, _v3

For example, compare:

- File name 1. interview02.docx
- File name 2. I_P02_R01_20180731.docx

File Name 2 includes:

- I = interview (type of data)
- P[n] = participant ID - participant 02
- R[n] = researcher ID – researcher 01
- Date of interview (YYYYMMDD) – 20180731

3. Integrity

How will you quality assure your data?

4. Confidentiality

How will you manage any ethical and Intellectual Property Rights issues?

Wherever possible personal/sensitive data should be encrypted to prevent unauthorised access. The most effective way to do this is to create an encrypted folder (also known as an encrypted container) and store files securely inside it.

Encryption software you can use:

Windows: 7zip for windows: works only on Windows computers, compatible with .ZIP format

Apple Mac: iZip for Mac OSX: works only on Apple Macs, compatible with .ZIP format
- Some users have reported crashing issues with iZip when using MacOS10.13 and 10.12.

Apple Mac: The Unarchiver for Mac OSX: works only on Apple Macs, compatible with .ZIP format

Apple Mac: an encrypted disk image : works only on Apple Macs

Veracrypt: works on any Windows, Apple Mac or Linux computers

The choice of encryption software should be standardised for all projects.

Where recording devices are used to capture/collect data, devices should be encrypted where possible. Once data has been uploaded to live storage, it should be deleted from all other devices.

Information on encrypting data files and devices can be found on the University of Edinburgh webpage: [Encrypting devices and documents](#).

5. Retention and Preservation

Which data do you plan to keep and for how long?

How will the data be preserved?

6. Sharing and Publication

Which data will be shared and how?

Are any restrictions on data sharing required?

9.2 RESPIRE Data Management Plan Guidance & Checklist

RESPIRE Data Management Plan Guidance

This guidance (and corresponding template) has six sections based on the University of Edinburgh Research Data Management Policy (<http://www.ed.ac.uk/is/research-data-policy>). For most questions we have provided a summary, basic guidance, and an example answer (taken from existing University of Edinburgh shared plans). Feel free to use information from your research protocol, but expand on the content for this detailed data management plan, as advised below. The guidance supports all projects: in development, live, and completed.

Responsibilities & Resources

Who will be involved in the data management of this research?

In summary: Give the names and roles for all the people involved in the creation and/or gathering of the data. You should also identify any other, non-human resources required.

Guidance: Throughout your data management plan you should explain the types of roles that will be involved in any aspect of your research data from collection, to management, to deposit and archiving. They could be responsible for implementing this plan.

You should consider any training required (e.g. [MANTRA course](#) or [Research Data Management coursera](#); hardware/software requirements (e.g. for storing data on your organisation's network storage or Edinburgh's DataStore¹); charges for data repositories (e.g. for any costs over a certain file size²); any costs and resources involved in preparing data for preservation/sharing (e.g. if you are not doing this yourself).

Data Capture

What data will be generated or reused in this research?

In summary: Describe the type, format, volume, and methods of data collection or creation; include details of any existing datasets to be used.

Guidance: Consider the types of data your research will generate, for example qualitative survey data, computational models, statistics, measurements, text, images, audio visual data, or samples.

Also consider the longevity of the file formats that you choose. Using open standards so your data can be read by a variety of software makes it easier to preserve and share with others.

If you are reusing third-party data, make sure you have sought appropriate permissions to allow for any data sharing or preservation plans.

¹ DataStore is a file store for active research data, and is available to all research staff and postgraduate research students (PGRs).

² Charges will be covered by RESPIRE for University of Edinburgh repositories only.

Example answer

“Every two days, we will subsample *E. affinis* populations growing under our treatment conditions. We will use a microscope to identify the life-stage and sex of the subsampled individuals. We will document the information first in a laboratory notebook and then copy the data into an Excel spreadsheet. For quality control, values will be entered separately by two different people to ensure accuracy. The Excel spreadsheet will be saved as comma-separated value (.csv) file daily and backed up to a server. After all data are collected, the Excel spreadsheet will be saved as a .csv file and imported into the program R for statistical analysis.”

Source: https://www.dataone.org/sites/all/documents/DMP_Copepod_Formatted.pdf

How much data will be generated?

Guidance:

- 0-50GB
- 50GB-250GB
- 250GB-500GB
- 500GB-2TB
- >2TB

Data Management

How will the data be documented to ensure it can be understood?

In summary: Documentation and metadata: information needed for data to be read and interpreted in the future (and where feasible reproduced), plan for collection or creation of this documentation and metadata, any metadata standards to be used. All metadata should be standardised using the metadata schema supplied.

Guidance: Producing good documentation and metadata provides context for your data, and makes it easier to find and use in the long term. The amount of effort put into documenting your data will depend on the intended lifespan and how widely you intend to share it.

You may want to capture details about what instrumentation has been used and how that has been calibrated, full variable and value labels, and details about your methodology. Consider preparing ReadMe documentation for each dataset. A ReadMe file is a simple text document (.txt) which sits alongside your data files and explains:

- What the data is;
- What the data covers;
- Where it the data can be found (file path);
- Licensing and access conditions (e.g. confidentiality requirements).

Imagine that you are preparing to publish your study findings. A reviewer asks to see your data in order to verify your findings. What information will that reviewer need to be able to:

- Find the data they need (folder location, file name);
- Open or access your data (format, software requirements, access conditions);
- Understand or interpret your data (field codes, abbreviations symbols, variables);
- Analyse your data (code, methods, outliers, missing data)?

ReadMe documentation should be standardised using a template.

Documentation could also include: lab notebooks and experiment protocols; questionnaires, codebooks, data dictionaries; software syntax and output files; database schema; methodology reports; provenance info about sources of derived data. More information is available in the MANTRA module on Documentation, metadata, citation (<https://mantra.ed.ac.uk/>).

Example answer

“Metadata will be tagged in XML using the Data Documentation Initiative (DDI) format. The codebook will contain information on study design, sampling methodology, fieldwork, variable-level detail, and all information necessary for a secondary analyst to use the data accurately and effectively”.

Source: ICPSR.

Where will the data be stored and backed-up?

In summary: describe where live data will be held, how will files be organised/ structured and named consistently, backup/recovery, security risks and how these will be mitigated, who will have access. If you will be collecting data in the field, how will this data be transferred securely?

Guidance: To prevent loss, unauthorised access, accidental deletion, etc., data should not be stored on desktop or laptop hard drives or portable media such as flash drives. Data should be stored on your institution’s networked storage.

The University of Edinburgh provides space on DataStore, which is maintained and supported by Information Services. DataStore is available via DataSync and ensures that the data are held securely. Data held on DataStore is automatically replicated to an off-site disaster facility and also backed up with a 60-day retention period, with 10 days of file history visible online.

A logical filing system should be set up (e.g. nested folders) with all folders and files clearly labelled. A standardised and meaningful file naming convention should be established for all folders and data files to make particular data files easy to find.

A file naming convention should include:

- No Special Characters: ""£\$%!~&*^()+=[{}~@:;#,<>
- Underscore Spaces: _ or %20 may replace the space
- Reverse Dates for sorting: YYYYMMDD • Version Control: Date_FileName_v1, _v2, _v3 For example, compare:
 - File name 1. interview02.docx • File name 2. I_P02_R01_20180731.docx

File Name 2 includes:

- I = interview (type of data)

- P[n] = participant ID - participant 02
- R[n] = researcher ID – researcher 01
- Date of interview (YYYYMMDD) – 20180731

Example answer

“The data will be stored on the University of Edinburgh DataStore. This is high quality, enterprise-class storage with guaranteed backup and resilience. The data is automatically replicated to an off-site disaster facility and also backed up with a 60-day retention period, with 10 days of file history visible online”.

Source: University of Edinburgh guidance.

Integrity

How will you quality assure your data?

In summary: describe the quality assurance processes that you will employ to ensure accuracy and consistency of your data.

Guidance: Explain how the consistency and quality of data collection will be controlled and documented. You should include calibration processes, repeat samples or measurements, standardised data capture or recording, data entry validation, peer review of data or representation with controlled vocabularies. More information is available in the MANTRA module on Organising data (<https://mantra.ed.ac.uk/>).

Example answer

“New data produced during the project will be derived from existing spatial and statistical datasets. These will be highly reliant on the quality assurance procedures of the agencies producing the original data. Information on the quality and reliability of the existing spatial data utilised by the project will be included in the SECRA meta-data. This will also indicate the data source and any procedures (either spatial or statistical) that have been applied to the data layers. If appropriate, statistical data showing the variation (standard deviation) in the data created will be included in the spatial database.

Data modelled by the project will be checked for internal consistency by the research team. This will involve sampling data for various points to check that any algorithm applied has produced the expected and desired outputs. The data will then, if appropriate, be checked against a similar or surrogate variable from another source to determine if the results are comparable with existing data from other agencies.”

Source: RELU Social and environmental inequalities in rural areas.

Confidentiality

How will you manage any ethical and Intellectual Property Rights issues?

In summary: Describe how you will address issues of ethical and legal compliance; including, details of consent needed for data preservation and sharing, steps to be taken to protect identity of participants, steps to be taken to ensure sensitive data is stored and

transferred securely, owners of the data, licenses for re-use, and restrictions for third party use. In order to prevent duplication, you may the project's reference ethics applications.

Guidance: Consider whether you will be creating any sensitive data that need to be kept confidential to protect participants or to safeguard Intellectual Property. If so, what procedures will you follow, for example obtaining permissions via consent agreements and data licenses, or protecting information via anonymisation, restricted access and embargo period?

More information is available in the MANTRA module on Storage and security (<https://mantra.ed.ac.uk/>).

Wherever possible personal/sensitive data should be encrypted to prevent unauthorised access. The most effective way to do this is to create an encrypted folder (also known as an encrypted container) and store files securely inside it.

Encryption software you can use:

- [Windows: 7zip for windows](#): works only on Windows computers, compatible with .ZIP format
- [Apple Mac: iZip for Mac OSX](#): works only on Apple Macs, compatible with .ZIP format - Some users have reported crashing issues with iZip when using MacOS10.13 and 10.12.
- [Apple Mac: The Unarchiver for Mac OSX](#): works only on Apple Macs, compatible with .ZIP format
- [Apple Mac: an encrypted disk image](#) : works only on Apple Macs
- [Veracrypt](#): works on any Windows, Apple Mac or Linux computers

The choice of encryption software should be standardised for all projects.

Where recording devices are used to capture/collect data, devices should be encrypted where possible. Once data has been uploaded to live storage, it should be deleted from all other devices.

Information on encrypting data files and devices can be found on the University of Edinburgh webpage: Encrypting devices and documents (<https://infosec.ed.ac.uk/how-to-protect/encrypting>).

Example answer

"Some consultancies or individuals may be reluctant to have their data shared. Such concerns will be resolved for the interviews and focus groups by ensuring all transcripts are anonymous and identifying detail (e.g. campaign names) are removed or given pseudonyms in the transcript.

The case analyses, industry awards data and analysis of promotional material will proceed on the basis of publicly available documents, so the issue of sharing should not arise. However, copyright may be an issue for some of these documents. To resolve this, and before data is stored by ESDS, copyright permission will be sought for web and other promotional material written by participating organisations". Source: Leeds RoadMaP.

Retention and Preservation

Which data do you plan to keep and for how long?

In summary: describe which data will be retained and shared/preserved; what length of time should the data be kept beyond the end of the project; where will it be archived.

Guidance: Consider which data are of long-term value and should be retained. You should keep the data needed to validate any published findings, and may wish to keep other data that could be reused.

How long do the data need to be kept? Check if you are subject to legal obligations or expectations from your funder. The UKRIO [Code of Practice for Research](#) (which has been adopted by the University of Edinburgh) recommends a minimum of 3 years.

Example answer

“Our intent is that the long-term high quality final data product generated by this project will be available for use by the research and policy communities in perpetuity. The raw supporting data will be available in perpetuity as well, for use by researchers to confirm the quality of the Mauna Loa Record. The investigators have made arrangements for longterm stewardship and curation at the Carbon Dioxide Information and Analysis Center (CDIAC), Oak Ridge National Laboratory (see letter of support)”.

Source: https://www.dataone.org/sites/all/documents/DMP_MaunaLoa_Formatted.pdf

How will the data be preserved?

Guidance: Consider how your data will be managed so it can still be opened and understood in several years' time, and who will do any work needed to ensure this? Will you offer your data for deposit in a subject-specific data archive in the Edinburgh DataShare repository

(<http://datashare.is.ed.ac.uk/>) or Edinburgh DataVault (<https://www.ed.ac.uk/is/datavault>)?

If you do not plan to use an established repository, the data management plan should demonstrate that resources and systems will be in place to enable the data to be curated effectively beyond the lifetime of the grant.

Example answer

“The University of Edinburgh undertakes to maintain the digital outputs of this project for the long-term and will utilise University infrastructure (namely the Edinburgh DataShare repository) to ensure preservation and continued access. Edinburgh DataShare is an online digital repository of multi-disciplinary research datasets produced at the University of Edinburgh, hosted by the Data Library in Information Services. It is a trusted repository, ensuring that research data will be preserved.”

Sharing and Publication

Which data will be shared and how?

In summary: Will the data produced by your project be made open?

If you answer Yes: How will you maximize data discoverability: conditions/ restrictions on sharing data (licenses or data sharing agreements), mechanism for sharing (via a repository), timing of data publication, arrangements for obtaining a persistent identifier.

If you answer No: Please explain why your data cannot be made open, e.g. costs/resources, ethical or commercial confidentiality or sensitivity.

Guidance: The University of Edinburgh provides its researchers (and their collaborators) two alternative services for sharing and archiving of data. DataShare is an open access repository and all data is freely available. DataVault is a restricted access archive controlled by the data owners and appropriate for sensitive information.

DataShare: is an open access repository where data will be held indefinitely. Datasets up to 100GB are accepted. All accepted submissions receive a permanent identifier (DOI) which can be used to site your dataset. The repository is optimised to be indexed by google scholar and google dataset search to promote data discovery.

DataVault, is a restricted access long term storage. Data is held encrypted and access to the data is restricted to nominated individuals. Datasets receive a DOI and the metadata is publicly available, promoting data discovery. This is not a permanent archive and depositors define how long the data should be retained. Data is reviewed for deletion at the end of the retention period. There is a fee for deposits over 100GB at the rate of £50 per 1TB per year.³

Further information on the [benefits of data sharing](#) is available on the RDM website.

Example answer

"The final data product will be released to the public as soon as the recalibration of standard gasses has been completed and the data have been prepared, typically within six months of collection. There is no period of exclusive use by the data collectors. Users can access documentation and final monthly CO2 data files via the Scripps CO2 Program website (<http://scrippsco2.ucsd.edu>). The data will be made available via ftp download from the Scripps Institution of Oceanography Computer Center. Raw data (continuous concentration measurements, weather data, etc.) will be maintained on an internally accessible server and made available on request at no charge to the user".

Source: https://www.dataone.org/sites/all/documents/DMP_MaunaLoa_Formatted.pdf

Are any restrictions on data sharing required?

Guidance: Not all data can be shared. You may not be able to share your data if:

- It has financial value or is the basis for potentially valuable patents;
- It contains sensitive, personal information about human subjects;
- It has not been consented by participants;
- Parts of the data are owned by others.

Outline any restrictions you need to place on data sharing, for example, if the data can only be shared under certain conditions or an embargo period is needed.

³ Fees will be covered by RESPIRE for UoE Repositories only.



Example answer

“Even though the final dataset will be stripped of identifiers prior to release for sharing, we believe that there remains the possibility of deductive disclosure of subjects with unusual characteristics. Thus, we will make the data and associated documentation available to users only under a data-sharing agreement that provides for (1) a commitment to using the data only for research purposes and not to identify any individual participant; (2) a commitment to securing the data using appropriate computer technology; and (3) a commitment to destroying or returning the data after analyses are completed.”

Source: NIH data sharing plan examples:

(http://grants.nih.gov/grants/policy/data_sharing/data_sharing_guidance.htm#ex).

9.3 RESPIRE METADATA: Template

RESPIRE METADATA: KEMHRC, INDIA

80 characters title amends

Ref	Partner's original title	Amended title
_001	Care-seeking practices of and barriers to care-seeking for pneumonia in children aged less than five years in tribal and non-tribal rural areas of Pune district, India	Care-seeking practices for childhood pneumonia in non/tribal areas of Pune India
_002	Development of spirometry predictive values for Indian population	ORIGINAL OK
_003	Assessment of ASHA's workload and its determinants	ORIGINAL OK
_004	Estimating Chronic Respiratory Disease (Asthma and COPD) burden in adults in Asian low and middle-income countries [4CCORD study - 4 Country ChrOnic	Estimating Chronic Respiratory Disease burden in adults in Asian LMICs
_005	To assess the feasibility of using a well-established teleconsultation facility (Micro-Health Centre -MHC) in management of COPD and Asthma in a resource constrained remote rural area	Teleconsultation in remote rural India: management of COPD and Asthma
_006	Practices & perceptions of public & private, general medical practitioners (primary care physicians: "GPs") in rural India for diagnosis & management of asthma & COPD	Asthma & COPD: practices & perceptions of public & private GPs in rural India
_007	Assessment of feasibility of introducing pulse oximetry in IMNCI services in primary health facilities in Pune district	Introducing pulse oximetry in IMNCI, primary health facilities in Pune India
_008	Formulating and testing a strategy for introducing Pulmonary Rehabilitation (PR) for COPD management in a rural Indian setting	Strategy introducing Pulmonary Rehabilitation for COPD management in rural India

9.3 RESPIRE METADATA Schema

Field Name	Field Value (please enter)	Guidance Notes
Identifier	UPM_PAAP_001	Please provide a local identifier used to identify the dataset (if available) -- this can be an acronym or a shortened version of the name used for reference
Title	Effectiveness of Pictorial Asthma Action Plan in Public Primary Care Clinics: A Randomised Controlled Study Effectiveness of Pictorial Asthma Action Plan in Public Primary Care Clinics: A Randomised Controlled Study	The name of the dataset
Abstract	This project aims to assess the effectiveness of a pictorial asthma action plan (PAAP) for adult patients with asthma in public primary care clinics in the Klang District, Selangor State, Malaysia.	Please provide a short paragraph explaining what the dataset contains and it's purpose.
Publisher	PAAP on behalf of the RESPIRE Collaboration	The organisation that is the data custodian. They are responsible for the data access request process, as well as publishing and maintaining the metadata for this dataset
Contact Point	RESPIRE@ed.ac.uk	Either a URL, or the contact details (name/email) of the person(s) who is responsible for the data access process for this dataset.
Access Rights	Access is managed on a project-by-project basis. Contact the RESPIRE team.	Text or link to website/documentation which gives guidance on the data access request process for this dataset.
Group		



Description	The burden of asthma remained a major public health issue in Malaysia, among the adult asthma patients, 68.0% visited their doctors for asthma attacks, 27.3% reported having a min of 6 (4-8) work-days loss and 69% did not have regular long-term follow-up. Asthma self-management is recommended in all major national/international asthma guidelines. An asthma action plan is an integral part of self-management education. It enables patients with asthma to adjust their own treatments according to changes in their disease. At present, in Malaysia, a non-pictorial written asthma action plan is used in clinical practice. A study conducted at public primary care clinics reported that about 60% of patients with asthma had limited health literacy. Pictorial asthma action plan (PAAP) has the potential to overcome the inequity of text-based asthma action plan (tAAP) and benefit all patients regardless of their health literacy. This project aims to assess the effectiveness of a pictorial asthma action plan (PAAP) for adult patients with asthma in public primary care clinics in the Klang District, Selangor State, Malaysia. For further information, see: https://usher.ed.ac.uk/respire/research/non-communicable-diseases/current/pictorial-asthma-action-plan Data Dictionary / Response Codes:	A free-text account of the data or a URL to a document (webpage, pdf, word) that describes the dataset. This should provide detailed context about the dataset so that a researcher can understand what data it contains and its purpose.
--------------------	---	--



	888 (Missing due to dropout): Used when data were not obtained because the participant withdrew or was lost to follow-up, resulting in missing values at subsequent timepoints. 999 (Not applicable): Item not answered because the question was not applicable for participants/not preferred to answer by participants."	
Release Date	LEAVE BLANK	The date of the latest release of the dataset. If this dataset is released regularly (e.g. quarterly), this information can be filled out in the periodicity field. Please input in the format YYYY-MM-DD.
Access Request Cost	LEAVE BLANK	Please provide a description of the cost, or an indication of the range/calculation of costs for processing a data access request.
Access Request Duration	LEAVE BLANK	Please provide an indicative value of the estimated typical processing time for a data access request.
Data Controller		Data Controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the way any Data Subject data, specifically personal data or are to be processed.
Data Processor		A Data Processor, in relation to any Data Subject data, specifically personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
License	The dataset will be deposited at the University of Edinburgh DataShare and/or Data Vault repositories.	A legal document under which the distribution is made available.
Derived Datasets	NOT APPLICABLE	Indicate if there are any derived datasets available. A derivation is a transformation of one dataset into another, an update of a dataset resulting in a new one, or the construction of a new entity based on a pre-existing entity.



Linked Dataset	NOT APPLICABLE	If applicable, describe other datasets that have previously been linked to this dataset and their availability. If no datasets have currently been linked, please indicate if there is a possibility to link the datasets as part of the data access request process.
Geographic Coverage	Malaysia	The geographical area covered by the dataset. This can be as specific (e.g. West London) or as broad (e.g. the United Kingdom) as required.
Periodicity	LEAVE BLANK	Please indicate the frequency of publishing and/or the rate the dataset is updated. E.g. Quarterly
Dataset end date	31/05/2026	The end date of the period that this dataset provides coverage for. Please use the format YYYY-MM-DD
Dataset start date	01/06/2022	The start date of the period that this dataset provides coverage for. Please use the format YYYY-MM-DD
Jurisdiction	Malaysia	Please use ISO country code for country under whose laws the data subjects' data is collected, processed and stored.
Population Type	Adults 18 years old and above with brnchial asthma and been prescribed with daily inhaled corticosteroids (ICS) for poor asthma control in the last year (according to Global Initiative for Asthma (GINA) Asthma Symptoms Control (2022) step 2 management for asthma control), in addition to as needed inhaled short-acting beta2-agonist (SABA); or as needed low dose ICS-formoterol for those on SMART therapy (Global Initiative for Asthma, 2022)	Please provide a description of the primary population type within the dataset (e.g. participants in a study, images with certain characteristics, electronic health records)
Statistical Population		Please provide the primary population size within the dataset, e.g. x number of participants in a study, y number of images with certain characteristics, health records for z number of patients



Age Range	to be provided later	Please specify what the age range of the population of the dataset is.
Physical Sample Availability	YES	Availability of the physical samples associated with the dataset as Yes or No. If this dataset has no associated samples or this column is not applicable to your dataset, please leave this field blank.
Keywords	RESPIRE; Malaysia;bronchial asthma; asthma action plan; self management; primary health care	A set of comma-separated 'keywords' or 'tags' used to associate this dataset with other datasets that are possibly similar.
Conforms to	LEAVE BLANK	If this dataset conforms to a standard such as OMOP or FHIR, please specify here.
Controlled Vocabulary	LEAVE BLANK	Standard terminology / Ontology / Controller Vocabulary used in the dataset such as ICD-10 codes, NHS Data Dictionary or SNOMED CT International
Language	English	The language of the dataset. This refers to the natural language used for textual metadata (e.g. titles, descriptions) of the dataset or the textual values of dataset distribution



Format	CSV, PDF Format: CSV, XLSX, PDF File size: 2.3 MB (dataset files only) Associated Documentation Files: 1. File Name: PIS_Consent_quant_ Eng_PAAP_Pts_20230725_V2.pdf Title: Participant Information Sheet and Consent Form (Quantitative & Qualitative Study – Patients) Version: v2.0 Date: 25 Jul 2023 Language: English Study Context: PAAP – Patient Quantitative & Qualitative Component Document Type: PDF Access: Internal study documentation 2. File Name:PIS_Consent_quali_Eng_PAAP_HCP_20240313_v3.pdf Title: Participant Information Sheet and Consent Form (Qualitative Study – Health Care Professionals) Version: v3.0 Date: 13 March 2024 Language: English Study Context: PAAP – Health Care Professionals Qualitative Component Document Type: PDF Access: Internal study documentation 3. File Name: PIS_Consent_quali_Eng_PAAP_Pts_20240313_v1.pdf Title: Participant Information Sheet and Consent Form (Qualitative Study – Patients) Version: v1.0 Date: 13 Mar 2024 Language: English Study Context: PAAP – Patient Qualitative Component Document Type: PDF Access: Internal study documentation 4.File Name: RESPIRE2_DMP_PAAP_20230707_V2_1.pdf Title: Data Management Plan – RESPIRE2 PAAP Trial Version: v2.1 Date: 07 July 2023 5. File Name: PAAP_quant_ pts_180_20250127_v2.csv Study Context: Quantitative Data- RESPIRE2 Randomised Controlled Trial – Pictorial Personalised Asthma Action Plans (Malaysia) Version: v2 Document Type: CSV Date: 27 Jan 2025 Access: Internal study documentation	If multiple formats are available, please specify. The file format of the dataset distribution. E.g. CSV, SQL
---------------	---	--



File size	212 KB	Typical extract file size, e.g. "Typically 10GB" or "10-20GB". This can be a range. If the precise size is not known, an approximation can be used.
Creator	RESPIRE Collaboration	Please provide the text that you would like to be included as part of any citation that credits this dataset. This should be the entity responsible for producing this resource
Citations	Cheong, A. T. (Creator), Shariff-Ghazali, S. (Creator), Salim, H. S. (Creator), Mohamad, F. (Creator), Mohanty, T. (Data Manager), Alawa, V. (Data Manager), Lim, P. Y. (Creator), Lee, P. Y. (Creator), Hussein, N. (Creator), Hanafi, N. S. (Creator), Ramdzan, S. N. (Creator), Ramli, R. (Creator), Tan, S. F. (Creator), Nordin, N. (Creator), Mohamed Yusoff, F. (Creator), Aman, Z. (Creator), Wong, C. K. (Creator), Khoo, E. M. (Creator), Pinnock, H. (Creator) (12 May 2026). Effectiveness of Pictorial Personalised Asthma Action Plans in Malaysian Public Primary Care Clinics: A randomised controlled trial. Edinburgh DataVault. 10.7488/98645d78-cc6c-47fb-99e5-edcedd635675	Please provide a list of known key citations, if available. If there are any publications that reference, cite or otherwise point to this resource, please specify them here.
DOI	https://doi.org/10.7488/98645d78-cc6c-47fb-99e5-edcedd635675	Please provide a Digital Object Identifier (DOI) if available. If no DOI is available, please leave blank.

9.4 AUTHOR DATASET ReadMe Template

This readme file was generated on [YYYY-MM-DD] by [NAME]
<help text in angle brackets should be deleted before finalising your document>
<[text in square brackets should be changed for your specific dataset]>

GENERAL INFORMATION

Title of Dataset:

<provide at least two contacts>

Author/Principal Investigator Information

Name:

ORCID:

Institution:

Address:

Email:

Author/Associate or Co-investigator Information

Name:

ORCID:

Institution:

Address:

Email:

Author/Alternate Contact Information

Name:

ORCID:

Institution:

Address:

Email:

Date of data collection: <provide single date, range, or approximate date; suggested format YYYY-MM-DD>

Geographic location of data collection: <provide latitude, longitude, or city/region, State, Country>

Information about funding sources that supported the collection of the data:

SHARING/ACCESS INFORMATION

Licenses/restrictions placed on the data:

Links to publications that cite or use the data:

Links to other publicly accessible locations of the data:

Links/relationships to ancillary data sets:

Was data derived from another source?

If yes, list source(s):



Recommended citation for this dataset:

DATA & FILE OVERVIEW

File List: <list all files (or folders, as appropriate for dataset organization) contained in the dataset, with a brief description>

Relationship between files, if important:

Additional related data collected that was not included in the current data package:

Are there multiple versions of the dataset?

If yes, name of file(s) that was updated:

Why was the file updated?

When was the file updated?

METHODOLOGICAL INFORMATION

Description of methods used for collection/generation of data: <include links or references to publications or other documentation containing experimental design or protocols used in data collection>

Methods for processing the data: <describe how the submitted data were generated from the raw or collected data>

Instrument- or software-specific information needed to interpret the data: <include full name and version of software, and any necessary packages or libraries needed to run scripts>

Standards and calibration information, if appropriate:

Environmental/experimental conditions:

Describe any quality-assurance procedures performed on the data:

People involved with sample collection, processing, analysis and/or submission:

DATA-SPECIFIC INFORMATION FOR: [FILENAME]

<repeat this section for each dataset, folder or file, as appropriate>

Number of variables:

Number of cases/rows:

Variable List: <list variable name(s), description(s), unit(s) and value labels as appropriate for each>

Missing data codes: <list code/symbol and definition>

Specialized formats or other abbreviations used:

9.6 Standard operating Procedure (SoP) - Template

Title: Secure Qualitative Data Management for the Photovoice study

Project: Understanding the views and experiences of people living with chronic respiratory disease (CRD): an adapted Photovoice study

Site: VRHP, KEM Hospital Research Centre, Pune, India

Prepared by:

1. Dipali Dhamdhere, Project Coordinator, Photovoice Study, VRHP, KEMHRC, Pune
2. Tapas Kumar Mohanty, Informatics and Data Science Liaison Officer, NIHR Global RESPIRE Project

Version: 1.1/ 31 Oct. 24

Objective:

This document encapsulates the steps for securely managing and accessing encrypted qualitative research data related to the NIHR RESPIRE-funded Photovoice study at VRHP, KEMHRC Pune. It ensures data confidentiality, integrity, and compliance with the EU/UK GDPR and the DPDP Act 2023 of India.

Scope:

This procedure applies to all research personnel involved in the RESPIRE Photovoice study at VRHP, KEMHRC Vadu, for handling and accessing qualitative data, ensuring proper encryption, secure access, and safe storage of data, password management, collaborative work on sensitive files, continuous training and the risks of emerging technologies such as AI/LLMs

1. Data Encryption and Password Protection

All qualitative data files must be encrypted using appropriate encryption tools (e.g., **VeraCrypt**) to safeguard sensitive information.

- **File Storage Location:** Store files in a designated encrypted folder on the system and while using an external encrypted drive along with the site-specific secure server.
- **Password Management:**
 - Use strong passwords (minimum of 20 characters with alphanumeric and special characters) for data encryption.
 - Passwords must be securely stored and shared only with authorised personnel (PI, Co-I, and Data Manager) through a password manager (e.g., KeePass).
 - Additionally, passwords for encrypted containers should be shared via a 7-Zip file encrypted separately, with the password for the 7-Zip file shared through WhatsApp (end-to-end encrypted and set to auto-delete) for added security.

2. Data Backups

- **Local Backup:** Weekly backup to an encrypted container on the secure server at VRHP, with a mirror server backup at KEMHRC, Pune.



- **Cloud Backup:** Encrypted data is further uploaded weekly to the institute's AWS secure cloud server, adding a layer of redundancy against data loss due to technical failures or unforeseen circumstances.

3. Security of the Devices

- **Physical Security:** All devices used for data collection (tablets, smartphones, audio recorders, portable drives, flash drives) are to be stored in a secure area with restricted access. Only the Project Coordinator, PI, and Co-I are authorised to access this area.
- **Daily Download and Secure Storage:** Data (e.g., photographs/audio) captured/collected on devices must be downloaded daily onto the official laptop, stored in an encrypted container, and securely backed up following the data backup protocols.

4. Accessing Encrypted Files

To access encrypted data files, follow these steps:

- **Step 1:** Open **VeraCrypt** on your computer.
- **Step 2:** In the search bar, locate the encrypted file by selecting the folder where the file is stored.
- **Step 3:** Select the encrypted file and click **Open**.
- **Step 4:** Enter the decryption password.
- **Step 5:** Select a VeraCrypt volume (e.g., Local Disk M:) where the file will be mounted.
- **Step 6:** Click on **Mount**. Enter the password again when prompted and click **OK**.

Once the encrypted file is mounted and available:

- **Step 7:** Minimise the VeraCrypt window.
- **Step 8:** Navigate to the newly mounted drive (e.g., Local Disk M:) and find the decrypted folders and files.
- **Step 9:** Open the file and manage or review data as needed for research purposes (e.g., interviews, transcripts, audio recordings).
- **Step 10:** Ensure that any modifications or updates to the data are saved in the same encrypted volume before unmounting.

After accessing and working with the data, the following steps must be followed to ensure secure closure:

- **Step 11:** Navigate back to VeraCrypt.
- **Step 12:** Click on **Dismount** to close the mounted disk.
- **Step 13:** The file will automatically be secured and encrypted again.

5. Collaborative Transcription and file sharing:

- **Use of MS SharePoint:** For collaborative transcription and real-time analysis, KEMHRC's MS SharePoint platform should be used. Access permissions will be restricted to authorised personnel, allowing secure collaborative work on transcription files.
- **File Sharing and Storage:**



- Restricted shared Word and Excel documents will be used to prevent unauthorised access and maintain file integrity.
- Once the transcription is completed, files will be deleted from the encrypted containers on personal devices.

6. Continuous Training and Weekly Meetings

- **Initial Training:** All research personnel, including Field Research Assistants (FRAs), will undergo task-oriented training in Marathi covering all security protocols, including GDPR and DPDP Act 2023 compliance.
- **Weekly Meetings:** Regular team meetings will be held to address ongoing challenges, update team members on best practices, and review challenges the team is facing.
- **Risk Management for Emerging Technologies:** Potential risks from technologies like AI/ LLM will be discussed regularly, with guidelines on safe and ethical use incorporated into research practices.

7. Responsibilities

- **Project Coordinator:** Responsible for maintaining the security of the encryption passwords, verifying data access permissions, and ensuring regular updates to the SoP.
- **Research Personnel, including Field Research Assistants:** All personnel handling sensitive qualitative data must adhere to this SoP, ensuring no unauthorised access and following secure file management protocols.
- **PI/Co-I:** Responsible for overall adherence to this SoP and the secure password storage and to ensure compliance with all aspects of UK GDPR and the DPDP Act of India 2023.

N.B: This safety SOP is a part of the RESPIRE Photovoice DMP (V1.5, 5 Dec 2023) and adheres to the ethical guidelines for secure data handling in research.

RESPIRE Platform III: Open Science, Data & Methodologies

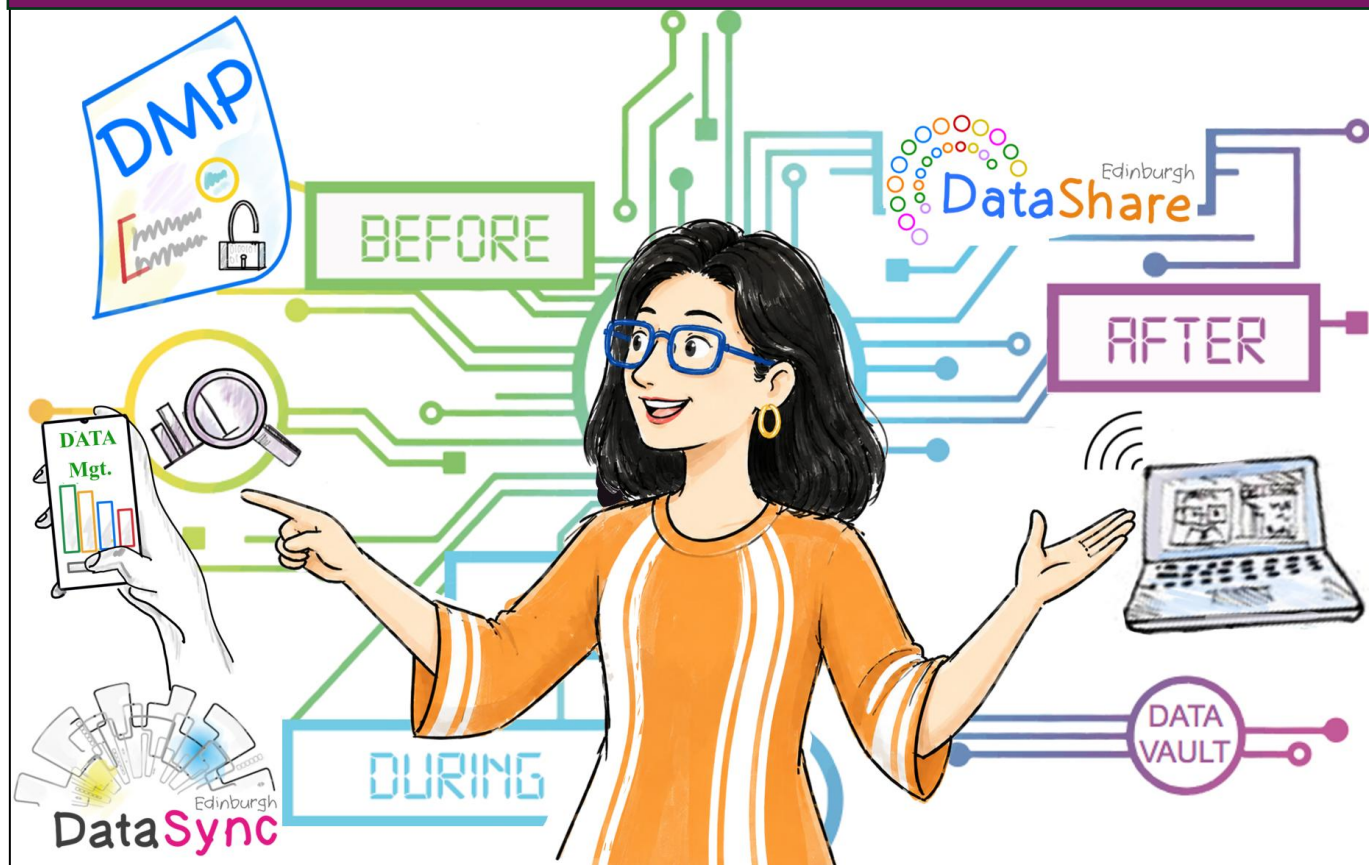


Illustration by Tapas Kumar Mohanty, concept inspired by the Library Services of the University of Edinburgh and the Usher Institute.



This work is licensed under [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) unless otherwise stated.



EDINBURGH DIAMOND | BOOKS

DOI: 10.2218/ED.9781836450764

ISBN (eBook) 978-1-83645-076-4



Led by:



THE UNIVERSITY
of EDINBURGH



UNIVERSITI
MALAYA

FUNDED BY

NIHR

National Institute for
Health and Care Research



UK International
Development

Partnership | Progress | Prosperity