Plan Overview

A Data Management Plan created using DMPonline

Title: Cultural Perceptions of Prehospital Emergency Care in Nepal. An Analysis of the Perceived Barriers to Providing and Accessing Emergency Medical Care.

Creator: First Namematt griggs

Principal Investigator: matt griggs

Data Manager: Dr Marie Bryce , matt griggs

Project Administrator: Dr Marie Bryce

Contributor: Dr Tom Gale, Dr Tracey Collett, Dr Ramesh Maharjan

Affiliation: University of Plymouth

Template: DCC Template

Project abstract:

Nepal’s Emergency Medical System (EMS) remains in the early stages of development, with limited access to prehospital emergency care (PHEC) due to resource constraints, challenging geography, and a fragmented healthcare system. While financial barriers to PHEC utilisation have been recognised, the cultural perceptions and social determinants influencing access and delivery remain poorly understood. This research aims to explore the perceptions of PHEC in Nepal, identifying perceived barriers to both providing and accessing emergency medical services.

Using a participatory qualitative research approach, the study will be conducted in three phases, across five geographically diverse study sites within Nepal: a metropolitan municipality (Kathmandu, Bagmati Province), two districts on the Terai (Bardibas, Madhesh Province and Bardiya, Lumbini Province), a hill district (Dhankuta, Koshi Province) and a remote mountain district (Humla, Karnali Province).

Phase One involves a scoping review of literature and policy analysis to evaluate existing PHEC provision within low and middle income countries (LMICs) in the region, alongside a workforce capacity review within the chosen study areas. Phase Two employs a survey and semi-structured interviews with PHEC workers and community members in the study regions to explore their perceptions, experiences, and challenges in accessing emergency care. Phase Three will apply a Nominal Group Technique (NGT) to engage stakeholders in developing culturally appropriate strategies to improve PHEC utilisation and effectiveness. Ethical approval is being sought in two stages, with stage one covering data collection in Kathmandu with the Nepal Ambulance Service and stage two the remaining study sites, once local stakeholder approval has been confirmed.

By examining sociocultural factors shaping PHEC access and delivery, this study aims to generate insights that can inform EMS policy, workforce development, and community engagement initiatives. The findings have the potential to contribute to Nepal’s ongoing emergency care system strengthening efforts, supporting the broader goal of achieving universal health coverage and improved emergency care access within Nepal.

ID: 172462

Start date: 01-10-2026

End date: 31-10-2030

Last modified: 14-08-2026

Copyright information:

The above plan creator(s) have agreed that others may use as much of the text of this plan as they would like in their own plans, and customise it as necessary. You do not need to credit the creator(s) as the source of the language used, but using any of the plan's text does not imply that the creator(s) endorse, or have any relationship to, your project or proposal

Cultural Perceptions of Prehospital Emergency Care in Nepal. An Analysis of the Perceived Barriers to Providing and Accessing Emergency Medical Care.

Data Collection

What data will you collect or create?

This research will generate data from a variety of sources, including:

Primary Data

- Surveys: Structured questionnaires capturing demographic data and health-seeking behaviours.
- Interviews: Audio recordings of semi-structured interviews with PHEC workers and community members during Phase 2.
- Group discussions: Audio recordings of Nominal Group discussions with PHEC stakeholders during Phase 3.
- Field Notes: Observational data recorded during interviews and stakeholder engagement meetings.
- Recruitment records: recruitment logs and an anonymous tally of approaches and declines maintained at each study site, held without any identifying information.
- Community advisory group records: notes of any advisory group meetings convened at each site, documenting their input into recruitment materials, the approach script and the appropriateness of interview topics.
- Consent records: signed consent forms, witness attestations for participants with low literacy, and records of any withdrawal request and associated data removal.
- Reimbursement and compensation records: records of travel reimbursement and compensation for time, held separately from research data and linked only by participant code.

Secondary Data

- Existing Literature & Policy Documents: Systematic review of academic literature, government reports, and healthcare policies related to PHEC in Nepal.
- Workforce & Resource Data: Data from official sources on EMS/PHEC workforce distribution, skill levels and available resources (where available) within the study areas.

Data types

- Audio Recordings: MP3/m4a or WAV files.
- Transcripts & Notes: Microsoft Word files/paper copies.
- Survey Data: password-protected Microsoft Excel or Word files/paper copies.
- Data Analysis files: MAXQDA files (.mx24)
- Translation and transcription files: produced offline using local transcription software held on an encrypted, University-managed device.

How will the data be collected or created?

The data for this study will be collected through a combination of primary and secondary sources:

Primary Data Collection

- Surveys: created electronically or on paper, with responses entered into a structured database to facilitate analysis at the earliest possible opportunity.
- Interviews: Conducted using a semi-structured guide to ensure consistency. Audio recordings will be translated and transcribed verbatim and cross-checked for accuracy.Audio recordings are captured on encrypted devices. English-language interviews are transcribed verbatim. Nepali-language interviews follow a two-stage process: initial transcription in Nepali, followed by English translation by the Research Assistant to preserve accuracy and cultural nuance. All translation and transcription is completed offline, using local software held on an encrypted, University-managed device, and no audio file is uploaded to, or processed by, an external or cloud-based service. Transcripts are cross-checked for accuracy by the Principal Investigator and the Research Assistant.
- Field Observations: principal investigator (PI) and research assistant (RA) will document observations during and around the interviews.
- Recruitment: participants are recruited both by self-referral in response to displayed recruitment materials and by direct in-person approach by the PI and RA at agreed public, community and workplace settings, following a standard approach script in Nepali. An anonymous tally of approaches and declines is maintained at each site to support reporting on recruitment and consideration of non-participation bias during analysis.

Secondary Data Collection

- Policy and Literature Review: Data will be drawn from published sources and grey literature, according to pre-defined inclusion and exclusion criteria.
- Existing Healthcare & Workforce Data: where possible, to be obtained from the Government of Nepal and/or gatekeeper organisations, ensuring alignment with national data standards.

Data Standards

- As participant data may include personal or high-value information classified as ‘Strictly Confidential – Level 1’, a high level of

security controls will be applied. Role-based access will be strictly limited to the Principal Investigator (PI), academic supervisors from the University of Plymouth and the Research Assistant, who is engaged by the University of Plymouth as a casual worker and who processes data solely on the instruction of, and under the supervision of, the PI within University of Plymouth systems. Access controls will be enforced throughout the entire data lifecycle, from creation to destruction.

- Data will be collected and stored in accordance with recognised national standards in both Nepal and the United Kingdom. In the UK, this will align with the University of Plymouth's Research Data Policy, Data Retention and Erasure Policy, and Data Protection Policy. In Nepal, data practices will comply with the National Ethical Guidelines for Health Research in Nepal (NHRC, 2022), which emphasise the importance of cultural sensitivity in data acquisition and protection, particularly for international researchers.
- The development of qualitative data collection tools will follow the Consolidated Criteria for Reporting Qualitative Research (COREQ) 32-item checklist, ensuring rigour and transparency in interview-based data collection.
- The project will follow the Data Documentation Initiative (DDI) standard for social science and health data, as it ensures a clear, detailed framework for describing research data.

Data Organisation and Management

- Naming Conventions: Files will follow a standardised structure, including date, participant/study ID, and data type (e.g. Interview_2025-03-06_Participant01.wav).
- Version Control: Versioning will be managed using University of Plymouth repositories and software. MAXQDA is being explored as the data analysis software.
- Folder Structure: Data will be stored in a structured hierarchy:
  - Raw Data (original files)
  - Processed Data (translated, transcribed and cleaned)
  - Analysis Files (coded transcripts, datasets)
  - Final Outputs (summarised results, reports)

Quality Control Measures

To ensure data consistency and reliability, the following procedures will be implemented:

- Principal investigator and research assistant will be appropriately trained to maintain consistency in data collection.
- Structured templates will be used to minimise data entry errors.
- Transcriptions and coded data may be reviewed by the director of studies and supervisors, with a subsample of transcripts independently coded by supervisors to verify analytical consistency and reduce bias.
- Consistent terminology and coding frameworks (Braun and Clarke's six phase framework) will be used to ensure integrity.

Documentation and Metadata

What documentation and metadata will accompany the data?

- Essential information for the different sets and subsets of data will include: data title, creators and contributors, date of creation, access conditions, methodology used and file type/format.
- All stakeholders will be engaged in the documentation process to ensure clarity and relevance, especially regarding cultural nuances and local practices that influence prehospital care perceptions and utilisation. This will ensure that the data generated will be accessible, comprehensible, and useful for future research and interventions.
- Documentation will also include the standard recruitment approach script, the recruitment flyer, and records of community advisory group input at each site, so that the conduct of recruitment and engagement can be reported transparently.
- Metadata for the project will follow the Data Documentation Initiative (DDI) standard for social science and health data, as it ensures a clear, detailed framework for describing research data.

Ethics and Legal Compliance

How will you manage any ethical issues?

How will you manage any ethical issues?

To ensure all ethical requirements are met, this project is to be approved by both the University of Plymouth Faculty of Health Research Ethics and Integrity Committee (FREIC) and the Nepal Health Research Council (NHRC). In particular this will be reviewed in terms of:

- Informed Consent: All participants (community members and PHEC workers) will be asked for explicit consent to preserve and share their data for future research purposes. The consent form will specify that anonymised extracts (including audio recordings, transcripts, notes, and survey data) may be disclosed in published works posted online for use by the scientific community. Participants will be informed that all other anonymised data will be stored securely within the University of Plymouth for ten years following the completion of the study, in accordance with its data management policy, and that access will be restricted to the

principal investigator and research team only. Participants will also be made aware that their anonymised data may be used to support related research within that period by the principal investigator or research team only. Consent for the use of pseudonymised transcripts in AI-assisted analysis is sought as a separate, optional item on the consent form; where a participant declines, their transcript is coded manually only and is excluded from any AI-assisted function, with no effect on any other part of their participation. Where a participant has low literacy, the participant information sheet and consent form are read aloud in full in Nepali and an impartial witness independent of the research team attests in writing that the information was read accurately and that consent was given freely.

- Protection of Participant Identity: All direct identifiers will be removed from the data to protect participant privacy. Data will be pseudonymised at the earliest opportunity and held in that form throughout collection, storage and analysis. Each participant will be assigned a unique code, which will be used instead of their personal details. A separate, secure key linking the codes to personal information will be stored in a different location to ensure confidentiality. Data is described as pseudonymised rather than anonymised for as long as the linking key is retained. All outputs are fully anonymised before publication or dissemination. Recruitment tallies are held without any identifying information.
- To further protect participant anonymity, particularly in rural or remote study sites where the risk of deductive disclosure is greater, gatekeeper organisations and districts will not be named or be made identifiable in any published outputs. Study site identifiers will be reported only at provincial level, with findings attributed to one of the following provinces: Bagmati (Kathmandu), Madhesh, Lumbini, Koshi, or Karnali (study site confirmation pending). Where direct quotations are used, any details that could identify an individual participant or their location will be removed or sufficiently generalised prior to the PhD submission or in any publication.
- Data Encryption: All sensitive data, including interview transcripts, recordings, and survey responses, will be stored on secure, password-protected servers within the University of Plymouth's OneDrive system. Only authorised personnel will have access to the data.
- Data Sharing: The Nepal Ambulance Service, the Nick Simons Institute and the Nepal Disaster and Emergency Medicine Center (NADEM) act as collaborating partners, supporting access to study sites, stakeholder engagement and the dissemination of findings. No collaborating organisation holds, accesses or processes study data at any stage and none has a data protection role in the study. No study data is shared with any collaborating organisation.
- Data Retention: Data will be retained for the duration of the project and for a specified period after the completion of the research (10 years) for potential future studies in line with the University of Plymouth data storage policy. After this period, all data will be securely destroyed, ensuring compliance with institutional and international data protection laws.
- AI tools: No identifiable participant data enters any AI system at any stage of this study. Interview audio is captured on encrypted devices and is translated and transcribed offline, using local transcription software held on an encrypted, University-managed device. Audio files are never uploaded to, or processed by, an external or cloud-based service.
- AI-assisted functions within MAXQDA (AI Assist) may be used only after transcripts have been pseudonymised and coded, and only to support interactive data exploration and the generation of suggested coding frameworks alongside researcher-led manual coding. These functions are optional, are not enabled by default and all AI-generated output is labelled as such within the software. Project files are held only on the Principal Investigator’s encrypted University-managed laptop and the software provider has no access to them. Where an AI function is invoked, only the minimum text necessary is transmitted under TLS 1.2 encryption to the provider’s GDPR compliant cloud server in Frankfurt and from there to its GDPR compliant AI subprocessor on servers within the EU. The provider (VERBI GmbH) states that its AI subprocessors delete the data after processing, do not permanently retain it and do not use it for model training, and maintains a published list of subprocessors.
- The English versions of all participant-facing documents were provisionally translated into Nepali using an AI large language model and verified by a Nepali speaker. No participant data, and no institutional or service data, was involved at any point in this process. All such documents are further validated by the incoming Research Assistant before distribution.
- The use of any AI tools requires approval from the University of Plymouth, the Nepal Health Research Council (NHRC) and the Faculty of Health Research Ethics and Integrity Committee (FREIC), and proceeds only with the separate, optional consent of the participant.

Roles and Responsibilities

In accordance with Data Protection Legislation, Matthew Griggs (PI) will act as the Data Controller for all participant personal data collected during this project, holding responsibility for determining the purposes and means of processing. The University of Plymouth provides the systems and infrastructure for the study. The Research Assistant is engaged by the University of Plymouth as a casual worker and processes data solely under the direct instruction and supervision of the Principal Investigator, within University of Plymouth systems. Access to study data is governed by the University’s information security and confidentiality requirements. Access is strictly limited to the Principal Investigator, the Research Assistant (only under direct supervision of the PI) and the academic supervisors throughout the data lifecycle. All data is held within the University of Plymouth OneDrive throughout and is not copied, exported or transferred to any external system or third party organisation. The data being processed includes: audio recordings, transcripts and notes, survey data, recruitment records and consent records.

How will you manage copyright and Intellectual Property Rights (IPR) issues?

As sponsor for the project, the University of Plymouth will own the copyright and IPR of any data collected and created.

Storage and Backup

How will the data be stored and backed up during the research?

- All sensitive data, including interview transcripts, focus group recordings, and survey responses, will be stored on secure, password-protected servers within the University of Plymouth's OneDrive system. Only authorised personnel will have access. OneDrive provides sufficient storage capacity and automatically backs up data as it is created. Interview recordings are transferred to the secure University of Plymouth OneDrive within 48 hours of collection and deleted from portable devices thereafter.
- In regions with limited internet connectivity, data will be temporarily stored on encrypted hardware approved and provided by the University of Plymouth, such as an encrypted USB storage device or voice recorder. Data will be uploaded to OneDrive at the earliest possible time and deleted from the device thereafter.
- Any physical copies of data, such as printed materials, will be minimised and held solely by the principal investigator. These will be scanned into a digital format at the earliest possible time, stored as described above, and securely destroyed to ensure compliance with institutional and international data protection laws.

How will you manage access and security?

Electronic

- All sensitive data, including interview transcripts, recordings, and survey responses, will be stored on secure, password-protected servers within the University of Plymouth’s OneDrive system. This will also include MAXQDA files (.mx24) used during data analysis. OneDrive offers sufficient storage capacity and automatic data backup. In accordance with the University’s data management guidelines, all electronic data will be retained for 10 years following project completion.
- In regions with limited internet connectivity, data may need to be temporarily stored on encrypted hardware approved and provided by the University of Plymouth, such as an encrypted USB storage device or voice recorders. Data will be uploaded to OneDrive at the earliest possible time and then permanently deleted from the device thereafter.

Paper/Hard copies

- Physical copies of data, such as printed materials, may be required at remote study sites or in settings with reduced literacy levels. Retention of these materials will be minimised and managed solely by the Principal Investigator (PI). Wherever possible, data will be digitised promptly, either scanned or manually entered into a secure OneDrive database, ideally on a daily basis. In the event that hard copies must be retained for longer periods, they will be stored in a locked facility or kept securely with the PI when in use or in transit. All physical data will be securely destroyed once digitised to ensure compliance with institutional policies and international data protection regulations.

Data Access and Security

- Access Management: Only the research team (PI, the RA and academic supervisors) will have full access rights to data files (audio recordings, transcripts & notes, survey data). Two-factor authentication will control access to data in OneDrive.
- Secure Data Sharing: All study data is held within the University of Plymouth OneDrive and accessed in place by the research team through role-based permissions. Data is not copied, exported or transferred to any external system, organisation or third party, and no cross-border file transfers are required.
- Local Encryption: if necessary field data will be encrypted on secure devices until uploaded to OneDrive.

Risks and Mitigation

- Data Loss: Mitigated by use of OneDrive storage and encrypted hardware with regular uploads to OneDrive, with real-time backups once internet access is available.
- Unauthorised Access: Mitigated by password-protected OneDrive storage and encrypted USB drives for field data if needed.
- Physical Theft or Loss: Equipment may be lost or stolen. Mitigated by encrypted devices, remote wiping/tracking, and regular monitoring.
- All analysis tools within MAXQDA will be operated locally by the PI only, on an encrypted University-managed device (laptop), with the software maintained through regular updates, bug fixes, and patches. The ‘TeamCloud’ feature within MAXQDA will not be used, avoiding potential risks associated with cloud storage, third-party processing, and data transfer. No identifiable data will be uploaded (participants will be informed in the PIS and consent form that their pseudonymised data may be used within AI software, and that this consent is a separate, optional item that may be declined without affecting any other part of their participation). While some AI features in MAXQDA rely on third-party service providers, these are based in the EU and fully GDPR compliant.

Selection and Preservation

Which data are of long-term value and should be retained, shared, and/or preserved?

Data of long-term value is selected for preservation, stored securely and protected against unauthorised modification or destruction in line with the University of Plymouth data storage policy. The following data will be retained for the duration of the project:

- Interview Transcripts: Essential for understanding cultural perceptions, these anonymised transcripts will be stored for long-

term access and can contribute to future research or policy discussions.

- Survey Responses: Quantitative insights that can be reused or further analysed in future studies, anonymised and stored for long-term access.
- Field Notes and Observational Data: Providing valuable context for interpreting other data, these will be linked to other datasets and carefully anonymised to protect participants' privacy.
- Ethical Consent Forms: Crucial for ethical compliance and potential future audits, these will be securely stored in accordance with institutional data retention policies.
- Data Documentation and Metadata: Documenting methodologies, instruments, and coding frameworks, this will provide context for the data and ensure its usability in future research, preserved alongside the data.
- Recruitment and Community Engagement Records: anonymous recruitment tallies and community advisory group notes, retained to support transparent reporting on recruitment, non-participation bias and the influence of community engagement on the study.

What is the long-term preservation plan for the dataset?

Data is stored securely and protected against unauthorised modification or destruction for the duration of the project and for 10 years after its completion, in line with the University of Plymouth data storage policy. Published articles and the final PhD thesis will be archived in the University research repository PEARL (Plymouth Electronic Archive and Research Library) for long term preservation. All other research data will remain within the University of Plymouth OneDrive, with access restricted to the research team throughout the retention period. Data will not be deposited in external or third-party repositories.

Data Sharing

How will you share the data?

Throughout the duration of the project, secure data will be shared between the Principal Investigator (PI), the Research Assistant (RA), and academic supervisors within the University of Plymouth OneDrive. Access is governed by the RA’s contract of employment with the University, the University’s information security and confidentiality requirements, and the ethical approvals held for the study, ensuring compliance with ethical guidelines, data protection legislation and institutional policies. The following arrangements apply:

- Access Control: As Level 1 strictly confidential data from outside the European Economic Area is being generated, data access will be restricted to authorised personnel only through secure, role-based permissions through a project SharePoint site.
- Data Sharing Scope: Only anonymised, aggregated data (e.g. survey responses, key findings from interviews) will be shared. Sensitive data will not be shared without proper consent.
- Sharing Format: Data will be shared within the research team in secure formats, i.e. encrypted files on OneDrive.
- Data will be stored and made available for sharing for a period of 10 years following the project's completion, in accordance with the University’s data management guidelines.
- Third-Party Sharing: No study data is shared with any external collaborator, institution or third party. Data is not copied, exported or transferred outside University of Plymouth systems at any stage, and collaborating organisations have no access to study data.

Sharing of findings

- Findings will be made available to all project stakeholders after the project’s conclusion and at points during the project’s duration where emergent themes and preliminary observations contribute to the project's overall aims (Phase 3).
- Project findings will be shared publicly through academic publications, conference presentations, and the University of Plymouth’s open access institutional repository, PEARL (Plymouth Electronic Archive and Research Library).
- A project website and social media platforms may be developed for promotional purposes.
- Findings are returned to participating communities through translated plain-language summaries and, where practicable, facilitated feedback meetings at each site, and to collaborating organisations including NADEM, the Nepal Ambulance Service, Tribhuvan University Teaching Hospital, the Nick Simons Institute and district health offices, to support translation into local service planning and policy. Only anonymised findings are shared in this way; no underlying study data is released.

Are any restrictions on data sharing required?

As Level 1 strictly confidential data from outside the European Economic Area is being generated, data access will be restricted to authorised personnel only through secure, role-based permissions through a designated OneDrive file with communication through Microsoft Teams. No study data is shared outside the research team, and no data is deposited in external or third-party repositories.

Responsibilities and Resources

Who will be responsible for data management?

The PI will be responsible for implementing the Data Management Plan (DMP), ensuring it is regularly reviewed and revised as needed. Specific data management activities will be assigned as follows:

- Data Collection & Storage: the PI and RA will collect data following ethical protocols, with secure storage managed by the University of Plymouth.
- Data Security & Access Control: The PI will oversee access permissions and ensure compliance with security measures.
- Data Sharing & Documentation: The research team will manage data anonymisation, metadata documentation and sharing of any published articles and the final PhD thesis through the PEARL Repository.

The persistent identifier for all datasets for the duration of the project will be the PI.

The Nepal-based supervisor, Dr Ramesh Maharjan, provides in-country oversight during fieldwork and advises on data collection within Nepal to ensure adherence to local requirements. Collaborating organisations, including NADEM, the Nepal Ambulance Service and the Nick Simons Institute, support site access, stakeholder engagement and dissemination only and have no data management role.

University of Plymouth will manage secure data storage, processing, and long-term archiving.

What resources will you require to deliver your plan?

All storage and repository systems are provided by the University of Plymouth with no additional costs needing to be covered by the PI or research team.

A data management training course provided by the University of Plymouth has been completed by the principal investigator in drawing up this plan.