Assessment Information

[CoreTrustSeal Requirements 2017–2019](#)

Repository: Qualitative Data Repository
Website: https://qdr.syr.edu
Certification Date: 29 November 2018

This repository is owned by: Maxwell School, Syracuse University

Qualitative Data Repository

Notes Before Completing the Application

We have read and understood the notes concerning our application submission.

True

CORE TRUSTWORTHY DATA REPOSITORIES REQUIREMENTS

Background & General Guidance

Glossary of Terms

BACKGROUND INFORMATION

Context

R0. Please provide context for your repository.

Repository Type. Select all relevant types from:

Domain or subject-based repository

Comments

The Qualitative Data Repository is a curated domain repository for data collected or generated through qualitative and multi-method research in the social sciences and cognate disciplines.

Links:
QDR Mission (on homepage): https://qdr.syr.edu

Brief Description of the Repository's Designated Community.

QDR serves a global social science community and especially those researchers working with qualitative methods and data. Given the relative novelty of sharing qualitative social science data, especially in the US context, QDR's staff actively engage in training researchers, providing in-person workshops (e.g., at the annual meeting of the American Political Science Association and the annual Institute for Qualitative and Multi-Method Research) as well as remote instruction via webinars.

Links:
Shourt courses directed by QDR staff at the American Political Science Association's Annual Meeting:
https://www.maxwell.syr.edu/moynihan/cqrm/Short_Courses_at_APSA/
Shourt courses directed by QDR staff at the international Institute for Qualitative and Multi-method Inquiry:
https://www.maxwell.syr.edu/uploadedFiles/moynihan/cqrm/IQMR%202018%20schedule%20and%20readings.pdf
QDR Webinar on data management: https://qdr.syr.edu/qdr-blog/webinar-securely-managing-qualitative-data (QDR staff organizes or participates in similar webinars regularly)

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

Level of Curation Performed. Select all relevant types from:

C. Enhanced curation – e.g. conversion to new formats; enhancement of documentation

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

Comments

During curation, QDR adds extensive metadata to data and files, converts file formats, and advises depositors with regard to respecting relevant ethical and legal limitations on data sharing (de-identification, copyright).

Links: QDR Curation policy: https://qdr.syr.edu/policies/curation

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

Outsource Partners. If applicable, please list them.

Amazon Web Services (servers and storage)

California Digital Library: DOI minting (likely soon to change to Datacite)

Reviewer 1

Comments:

Accept

Other Relevant Information.

QDR is the only repository with a sole focus on qualitative social science data in North America. It is part of Data-PASS, the data preservation alliance for the social sciences (discussed in detail below).

ORGANIZATIONAL INFRASTRUCTURE

I. Mission/Scope

R1. The repository has an explicit mission to provide access to and preserve data in its domain.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Response:

QDR's mission statement is displayed on our homepage at qdr.syr.edu:

"QDR curates, stores, preserves, publishes, and enables the download of digital data generated through qualitative and multi-method research in the social sciences. The repository develops and disseminates guidance for managing, sharing, citing, and reusing qualitative data, and contributes to the generation of common standards for doing so. QDR's overarching goals are to make sharing qualitative data customary in the social sciences, to broaden access to social science data, and to strengthen qualitative and multi-method research."

QDR's mission statement is promoted on our webpage as well as in our institutional report, QDR Access and provides the foundation for our policies and governance.

Links:
QDR Mission (on homepage): https://qdr.syr.edu
QDR Access: https://qdr.syr.edu/qdr-publications/qdr-access

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

II. Licenses

R2. The repository maintains all applicable licenses covering data access and use and monitors compliance.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
Accept.

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository

Response:

QDR data are governed by a set of agreements between QDR and depositors (Standard Deposit Agreement), between QDR and downloaders (Standard Download Agreements), and by our General Terms and Conditions of Use. Their content is described in detail below. Currently, QDR disseminates none of its data under an open license (such as CC0 or CC-BY). This decision, based on advice from similar repositories such as UK Data, reflects the particular sensitivity of much qualitative data. We constantly re-evaluate this policy to assure it serves the interest of our depositors, the human participants involved in the data projects that are deposited with us, as well as QDR's stakeholders in the research community. We may in the future selectively apply open licenses to suitable data in consultation with their owners/depositors.

As part of the standard deposit agreement, depositors grant QDR all rights required to perform curation and preservation tasks on the data, specifically (drawn directly from the text of the agreement):
- "To disseminate copies of the data project in a variety of media formats
- To promote and advertise the data project in any forms or media
- To describe, catalog, validate and provide documentation about the data
- To store, translate, transfer, move, copy and re-format the data in any way to ensure its future preservation and accessibility
- To incorporate metadata and documentation for the data project into public access catalogs.
- To enhance, transform and/or re-arrange the data project, including the data and metadata, in order to protect respondent confidentiality, improve usability, or to facilitate any task listed [...] above."

As part of our standard download agreement, researchers agree to use data only for research and teaching and to not attempt to re-identify individuals in de-identified data. The download agreement also bars the unauthorized redistribution of data, requires proper attribution during its use, and lists possible consequences for violating the agreement, which include possible bans from future use of QDR, reports to both institutional and federal bodies regulating research ethics, and potential legal action.

As part of a special deposit agreement, depositors can specify additional access conditions that can regulate who may access the data, and to which users need to explicitly agree (by signing a special download agreement) before downloading. Such access conditions are adjusted to reflect both the sensitivity of the data and the risk for re-identification and are custom-created in close communication with the depositor. Internally, restricted data are handled using specific protocols as specified under R4.

Links:
General Terms and Conditions: https://qdr.syr.edu/termsandconditions
Standard Download Agreement (requires registration): https://qdr.syr.edu/discover/standarddownload
Standard Deposit Agreement (requires registration): https://qdr.syr.edu/deposit/standarddeposit
Special Deposit Agreement (requires registration): https://qdr.syr.edu/deposit/specialdeposit
Access controls: https://qdr.syr.edu/guidance/human-participants/access-controls

III. Continuity of access

R3. The repository has a continuity plan to ensure ongoing access to and preservation of its holdings.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Response:

QDR is committed to providing repository services and access to data for the long term. Cognizant that funding and institutional environments can change, QDR has taken various measures to ensure continued access to its materials in the event of cessation of operations, within the scope of its commitment to provide access to data for at least 20 years from the point of deposit. Beyond QDR's strategies for sustainability (R5) and preservation (R14), the repository assures continued access to its material via membership in two organizations, the Data Preservation Network (DPN, https://dpn.org/) and the Data Preservation Alliance for the Social Sciences (Data-PASS, http://www.data-pass.org/).

As part of our agreement with DPN: (1), our holdings are deposited in DPN's long-term storage facility, which guarantees preservation for 20 years, and (2), DPN will seek out a new custodian for the data should QDR not be able to assure continued access after the guaranteed preservation period.

Data-PASS follows a similar, but more immediate and guaranteed succession rule. If any of Data-PASS's member repositories ceases operations, the other members agree to continue hosting its materials.

QDR's deposit agreement explicitly allows QDR to transfer stewardship of deposits to ensure ongoing access.

Links:

Data-PASS: http://data-pass.org/

DPN: https://www.dpn.org/

Standard Deposit Agreement (requires registration): https://qdr.syr.edu/deposit/standarddeposit

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

IV. Confidentiality/Ethics

R4. The repository ensures, to the extent possible, that data are created, curated, accessed, and used in compliance with disciplinary and ethical norms.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository

Response:

Ethical research and data practices are of concern to all researchers. They can be of particular concern to qualitative researchers who have long-established relationships of trust with research participants. As part of QDR's curation protocol, for all data projects that include data gathered from human participants (such as interview transcripts), QDR

requests and reviews IRB/ethics board approval and the informed consent language used during the research to help the depositor evaluate if the sharing of data is precluded, and/or to aid the depositor in respecting any limits on the sharing of data that result from guarantees made to project participants.

Where deposited data are de-identified, curators review all documents to help depositors decide whether de-identification has been carried out properly. Where data and related documentation are in a language in which no member of the QDR staff is proficient, curation staff uses automated translation to spot check de-identification and conveys best de-identification practices to depositors. In all cases, QDR's role is advisory. The final responsibility for decisions concerning de-identification remains with depositors.

During initial consultation with depositors, QDR staff also help the depositor to assess the sensitivity of data and potential disclosure risks and aids the depositor in identifying appropriate levels of access controls ranging from access for all registered users to access only on-site. Details of available access conditions are described in the documentation of access conditions.

For sensitive data, QDR follows strict protocols for transmitting, handling, and storing data. Depositors are instructed to encrypt data using AES-256 encryption prior to transfer, using SFTP or a Dropbox business folder with multi-factor authentication enforced for all users able to access content. Sensitive data are stored using AES 256 encryption.

Where the depositor requests additional safeguards for sensitive data, we help them to decide which access conditions should be imposed so that the data can be downloaded, The data are then distributed under a Special Download Agreement reflecting those access conditions. The conditions specified in the agreement reflect the nature of the disclosure risk in the data and can contain, for example, requirements for IRB/ethics board approval and/or a data security plan.

Sensitive data requires responsible use. QDR ensures that data is only released to personally identified individuals: access to data is granted following authentication via institutional e-mail and videoconferencing.

Additional requirements for data use are specified in the special download agreement and follow both depositor requests and QDR's assessment of the identifiability and risk for human participants of the data in question. The general requirements, by level of sensitivity, are outlined in QDR's "Handling Sensitive Data" policy under "Access to Restricted Data". For low sensitivity restricted data, authentication, a research plan, and assurances to not distribute the data further are typically sufficient for access. For medium sensitivity data, QDR requires a detailed data security plan as well as IRB approval for the proposed research and, in additional to the depositor's signature, the signature of an authorized institutional representative on the special download agreement. For highly sensitive data, QDR only allows access in person in a monitored room and screens users' notes. (While QDR does have the capacity to provide such access, it does not currently hold any data it classifies as highly sensitive). QDR is continuously exploring additional means of certifying researchers for access to sensitive data and thus facilitating access. We expect to be participating as a pilot institution in ICPSR's "Research Passport" initiative (see working paper linked below) that will leverage cross-repository collaboration to certify researchers in handling sensitive data.

Through its Terms and Conditions as well as its Standard Download Agreement, QDR also requires that researchers agree to use data ethically for data not deemed sensitive. As outlined, this includes giving attribution when using the data, not re-publishing it without explicit consent, and not using it for commercial purposes.

Given these precautions, we expect any misuse QDR's data to be rare. Should it occur, QDR's Download Agreements stipulate a range of sanctions for violation of the agreements, including deletion of user accounts, contacting the QDR institutional representative at the user's home institution (if that institution is a member of QDR) and the IRB at the user's home institution, and in cases endangering human participants, reporting to the federal Office of Human Research Protection.

QDR limits access of QDR staff to sensitive data. All access is overseen by senior staff, who have trained (and published) on the handling of sensitive qualitative data and regularly attend international workshops and conferences in data science and management to remain informed of state-of-the art practices and technology.

Links:
Standard Deposit Agreement (requires registration): https://qdr.syr.edu/deposit/standarddeposit
Standard Download Agreement (requires registration): https://qdr.syr.edu/discover/standarddownload
Handling sensitive data: https://qdr.syr.edu/policies/sensitivedata
Curation: https://qdr.syr.edu/policies/curation
Access controls: https://qdr.syr.edu/guidance/human-participants/access-controls
De-identification guidance: https://qdr.syr.edu/guidance/human-participants/deidentification
IRB guidance: https://qdr.syr.edu/guidance/human-participants/irb
ICPSR Whitepaper on Researcher Passport: http://hdl.handle.net/2027.42/143808

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

V. Organizational infrastructure

R5. The repository has adequate funding and sufficient numbers of qualified staff managed through a clear system of governance to effectively carry out the mission.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Response:

QDR is housed in the Center for Qualitative and Multi-Method Inquiry (CQMI), a unit of the Maxwell School of Citizenship and Public Affairs, a nationally leading public policy school at Syracuse University. CQMI is also the home of the Consortium for Qualitative Research Methods (CQRM), which conducts an annual international Institute for Qualitative and Multi-methods Research with around 180 participants.

The repository is led by social scientists at Syracuse University and Georgetown University as well as information scientists at the University of Washington at Seattle:

Directors:

Colin Elman, Professor of Political Science, Syracuse University.

Diana Kapiszewski, Associate Professor of Government, Georgetown University.

Technical Directors:

Carole Palmer, Professor and Associate Dean for Research, Information School, University of Washington, Seattle

Nic Weber, Assistant Professor, Information School, University of Washington, Seattle

QDR's Associate Director and Curation Specialist assist users and curate deposits with the support of two graduate student assistants as well as part-time support from CQMI personnel.

QDR has a small team of developers (one frontend/database, one systems/dev-ops), building on a lightly customized version of the Dataverse open source development software to reduce development costs.

QDR staff regularly attend professional meetings to present on their work and benefit from an international community of data specialists. Among conferences attended in the past two years are the annual meeting of the International Association of Social Science Information Services and Technology (IASSIST), Research Data Alliance (RDA), Dataverse Community Meetings, Research Data Access and Preservation Summit (RDAP), Preservation and Archiving Interest Group (PASIG), and the International Data Curation Conference (IDCC). QDR and/or its personnel are members and

actively participate in international bodies including RDA, IASSIST, and DCC. One of QDR's co-directors serves on the Center for Open Science's Transparency and Openness Promotion (TOP) Guidelines Coordinating Committee and until recently a co-director served on ICPSR's Governing Council. QDR's Associate Director serves on the Technical Steering group of DataCite.

Funding for the repository currently comes from various sources:
Grant funding for core operations provided by the National Science Foundation (Political Science Program)
Project-based funding by the Robert Wood Johnson Foundation
In-kind support by Syracuse University (office space, IT support, administrative support, graduate assistants)
Revenues from institutional membership and depositor support starting in July 2018. These are part of a long-term sustainability plan.

QDR has a robust, and increasing, user base. As of October 2018, QDR has over 1,400 registered users and the site receives an average of about 1,700 monthly unique users according to google analytics. Most users (ca. 70%) and visitors (ca 60%) are from the United States, but both groups include researchers from across the globe, spanning five continents.

Links:
Institutional Membership: https://qdr.syr.edu/membership/join
QDR Access: https://qdr.syr.edu/qdr-publications/qdr-access
Governance: https://qdr.syr.edu/about/governance
Contact/Personnel: https://qdr.syr.edu/contact

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

VI. Expert guidance

R6. The repository adopts mechanism(s) to secure ongoing expert guidance and feedback (either inhouse or external, including scientific guidance, if relevant).

Compliance Level:

4 – The guideline has been fully implemented in the repository

Response:

From its inception QDR has sought out and received advice from information and data science experts and its designated community of social scientists and other researchers. QDR has two advisory boards:

The Technical Advisory Board, whose members are specialists from libraries and data repositories, advises QDR on technical questions including development, curation, and digital preservation.

The Research Advisory Board, whose members are leading social scientists, assures that QDR serves the interests of its main constituency, practicing social scientists.

Each of these boards meets twice a year via teleconference. QDR also reports to both boards at the end of each quarter and solicits advice and feedback. For specific questions or major decisions, QDR seeks out the advice of board members individually.

In addition QDR regularly presents on its work at international conferences and workshops (see R5). To gain additional insights, QDR also organizes workshops convening diverse groups of international experts to focus on key concerns of archiving and curating qualitative social science data. Recent workshops have addressed archiving copyrighted material, sharing sensitive materials from research involving human participants, and curating data from computer assisted qualitative data analysis (CAQDAS) software popular with social scientists.

Finally, QDR personnel regularly teach data management to researchers, both in seminars and in individual consultations. These conversations serve as a constant check that the services offered address the needs and concerns of the repository's designated user community.

Link:

Advisory boards: https://qdr.syr.edu/about/governance

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

DIGITAL OBJECT MANAGEMENT

VII. Data integrity and authenticity

R7. The repository guarantees the integrity and authenticity of the data.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Response:

QDR follows the OAIS reference model in handling data.On receipt, QDR personnel check data files and metadata for completeness and integrity and, as needed, solicit updated or additional files from depositors. The complete initial deposit (Submission Information Package, SIP) is then committed to archival storage. It is also included in the data packages deposited with QDR's long-term storage partner (DPN), where file integrity is periodically monitored.

While there is no formalized identity check in place, QDR's curation team typically communicates directly by phone/skype with depositors and encourage the use of institutional emails for registration and communication. We are planning using ORCID for authentication.

On ingest, the Dataverse software automatically creates an MD5 checksum for every ingested file that allows for checking file integrity manually including by users and third parties. Files are stored on AWS S3, where redundant copies of each file are stored on distributed servers and integrity checks at rest are performed using content-MD5 checksums and cyclic redundancy checks (CRCs). AWS also performs integrity checks during data transfer.

The Dataverse software automatically enforces version updates on data for every change of published data using a two digit versioning system (e.g., 2.1). Small changes as well as changes to the metadata are recorded as minor changes, such as 2.1 to 2.2. Updates of data or other major changes receive a new version number (e.g., from 2.1 to 3.0).

Links:

Digital Preservation Network: https://www.dpn.org/

AWS S3 storage: https://aws.amazon.com/s3/faqs/

Digital preservation policy: https://qdr.syr.edu/policies/digitalpreservation

Curation policy: https://qdr.syr.edu/policies/curation

VIII. Appraisal

R8. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for data users.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Response:

QDR prioritize the acquisition and curation of deposits according to our collection development and appraisal policy. Under that policy, and following its mission, QDR prioritizes "qualitative data, or data associated with mixed-method research with a strong qualitative component, that are generated and/or used in the social sciences or cognate disciplines" and/or that hold "great intellectual value and/or that are of high quality." All data are reviewed by QDR's Associate Director or Curation Specialist. As qualitative data archiving is a relatively new field, community norms are not

yet well established or widely held. QDR largely follows the recommendations of the UK Data Archive for preparing qualitative data for archiving, and has also developed its own recommendations for data preparation and preferred formats.

QDR only requires depositors to complete a small number of metadata fields that provide basic bibliographic description of the data. However, QDR works closely with depositors to encourage and help them to provide in-depth documentation about the collection or generation and context of the data. Where metadata initially provided by depositors are too sparse to allow secondary users to make sense of the data (e.g., where no data collection methodology is described), QDR works with depositors to improve documentation. In line with the collection development policy, data that are found too lacking in documentation to be useful are not published. QDR curation staff, in collaboration with depositors, will convert detailed documentation into structured metadata. QDR's metadata application profile closely follows (a subset of) Data Documentation Initiative (DDI) Codebook, the de-facto standard for social science metadata. To the extent possible, metadata categories are linked to more generic vocabularies, specifically Dublin Core and the DataCite Metadata Kernel.

QDR staff converts files that are sub-optimal formats into preferred file formats during curation where possible. Where no suitable format for archiving exists, QDR archives files as they are and commits to bit-level preservation. QDR staff proofreads and systematizes documentation provided by depositors to generate rich, standardized metadata (see R9 for more on file formats, conversion, and metadata).

Links:

Data preparation guidance: https://qdr.syr.edu/guidance/preparing-data

Recommended file formats: https://qdr.syr.edu/guidance/managing/formatting-data

Collection development and appraisal policy: https://qdr.syr.edu/policies/collectiondevelopment

Metadata application profile: https://qdr.syr.edu/policies/metadata

UK Data file format recommendations: https://www.ukdataservice.ac.uk/manage-data/format/recommended-formats

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

IX. Documented storage procedures

R9. The repository applies documented processes and procedures in managing archival storage of the data.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository

Response:

QDR's data storage procedures are documented in its preservation and curation policies and follow the OAIS reference model. The main storage facilities of the repository are on AWS S3, which itself has significant protections against data loss such as redundant file storage across multiple data centers. In addition, QDR maintains on-site back-ups at Syracuse University, as well as long-term storage through the DPN (see R3). Both AWS and DPN perform regular file-integrity checks to guard against the failure of storage media. Full system back-ups are performed on AWS S3 daily and can be used for quick recovery in typical scenarios, with back-ups at Syracuse and DPN allowing recovery of data following a catastrophic event.

QDR's preservation policy is based on recommendations from the Library of Congress as well as other data repositories with significant holdings of qualitative data such as UK Data and DANS. Following receipt of a data deposit, files are converted to recommended storage formats and ingested into the Dataverse repository system. The file formats and types and file migration follow industry standards and recommendations. All changes are recorded in a readme file accompanying the data. QDR plans to record such preservation action in PREMIS metadata, but is not currently implementing that. All used file formats are monitored for obsolescence using the Library of Congress's Sustainability of File Formats pages (https://www.loc.gov/preservation/digital/formats/fdd/descriptions.shtml) as well as the UK National Archive's PRONOM service. Files in formats threatened by obsolescence are converted to suitable replacement formats.

Most files currently archived with QDR are not sensitive and do not require special security provisions. Sensitive materials are stored using AES 256 encryption on both AWS and local servers. All access to server software is controlled using virtual private networks.

Links:

Curation policy: https://qdr.syr.edu/policies/curation

Security and infrastructure: https://qdr.syr.edu/policies/security

Sensitive data: https://qdr.syr.edu/policies/sensitivedata

Digital preservation policy: https://qdr.syr.edu/policies/digitalpreservation

Reviewer Entry

X. Preservation plan

R10. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository

Response:

QDR's preservation policy describes the full preservation framework following the structure of OCLC's "Trusted Digital Repository" framework. As outlined in the policy, preservation of all files is guaranteed for a minimum of 20 years during which all efforts will be made to ensure permanent access to files. QDR assures access to files and content by using a file-format migration strategy as described in R9 and is committed to bit-level preservation where suitable preservation formats are not available.

The obligations of repository and depositor are clearly laid out in the Standard/Special Deposit agreement, at least one of which is signed by every depositor prior to the publication of data projects, marking the transfer of custody. The deposit agreement explicitly permits QDR to transform, duplicate, and disseminate the data (in the form of a non-exclusive license).

QDR's preservation actions are specified in both preservation and curation policy. An (annotated) copy of the curation policy is also used as an internal checklist for all data deposits to ensure adherence. QDR describes best practices for preparing data deposits in a dedicated guidance page on the QDR web site, and also works with depositors whose initial

deposit does not meet our internal standards.

Links:

Curation policy: https://qdr.syr.edu/policies/curation

Digital preservation policy: https://qdr.syr.edu/policies/digitalpreservation

Data preparation guidance: https://qdr.syr.edu/guidance/preparing-data

XI. Data quality

R11. The repository has appropriate expertise to address technical data and metadata quality and ensures that sufficient information is available for end users to make quality-related evaluations.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Response:

The quality of shared data depends upon their understandability and re-usability. These qualities, in turn, depend upon the organization of the data, and the clarity and completeness of the documentation that accompany them (i.e., how well they describe the data, the process through which they were collected/generated, and the context of their creation). QDR encourages depositors to provide all relevant information that allows for well-informed re-use of the data and works closely

with them to help them provide the highest possible level of data and documentation quality. This process relies on the subject-expertise of QDR's curation staff. Curation staff also assess the consistency of the data with the provided documentation and request changes, fixes, or updates from depositors as needed. Curation is supervised by senior staff all of whom hold graduate degrees in social science.

Metadata are generated in consultation with depositors using the Dataverse input mask, which maps (and exports) to Data Documentation Initiative (DDI) Codebook, the de-facto meta standard for social science, as well as other metadata formats such as DataCite XML and can be harvested using OAI-PMH. The actual cataloging of the metadata is performed by QDR curation staff based on depositor input and is subject to review by the depositor.

As part of the curation process, QDR also links to published work that uses or cites the data. The repository is closely following initiatives such as Scholarly Link Exchange (scholix) and Making Data Count and will use their output (for example, usage statistics) to provide additional links to related works and usage metrics together with dataset.

There is no formalized way for the designated community to comment or rate data or metadata. Nonetheless, QDR regularly works with scholars who re-use data in teaching and research in order to better understand their requirements and, if needed, adjust cataloging and curation practices.

Links:
Metadata application profile: https://qdr.syr.edu/policies/metadata
Curation policy: https://qdr.syr.edu/policies/curation
Collection development and appraisal policy: https://qdr.syr.edu/policies/collectiondevelopment

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

XII. Workflows

R12. Archiving takes place according to defined workflows from ingest to dissemination.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository

Response:

QDR's workflows in handling, storing, and preserving data and keeping it secure are described in the following documents:

- Preservation policy (describes conformance to OCLC's trusted digital repository and the OAIS reference model)
- Curation policy (supplements the preservation policy with a specific focus on QDR's activity to increase data and metadata quality and assure ethical sharing of data)
- Appraisal and Collection Development (describes QDR's criteria for accepting data)
- Sensitive data (describes the handling of different levels of sensitive data)
- Security (describes back-ups and security provisions)
- Standard/Special deposit agreements (formal agreement outlining depositor and repository rights and obligations at a high level of abstraction)

R8 describes QDR's appraisal procedures. Where data are found to not fit QDR's mission or the repository is otherwise unable to accept them, curators will actively assist the relevant researcher(s) in finding an alternative location for the data. Together with QDR's mission statement, the Appraisal policy specifies the types of data stored by QDR, i.e. data generated through and/or used in qualitative and multi-method research The diversity of such data complicates automated checking and analysis, which is why QDR relies heavily on its expert curation staff throughout the data lifecycle.

As described in R9, QDR describes its handling of data to depositors in an agreement that they sign (Standard deposit agreement) and provides additional details in its curation policy. The handling of confidential data is described above in R4 and in the "sensitive data" policy. When depositors wish to place restrictions on access to their data, these are specified individually in coordination with the depositor and codified in a set of special deposit/download agreements.

Transformation of data for archiving is described in the preservation and curation policies and in R9 above.

Security, audit, and back-up procedures are outlined in the Security document and R16.

Links:

Digital preservation policy: https://qdr.syr.edu/policies/digitalpreservation

Curation policy: https://qdr.syr.edu/policies/curation

Appraisal and collection development policy: https://qdr.syr.edu/policies/collectiondevelopment

Sensitive data: https://qdr.syr.edu/policies/sensitivedata

Security and infrastructure: https://qdr.syr.edu/policies/security

Standard deposit agreement (requires registration): https://qdr.syr.edu/deposit/standarddeposit

Special deposit agreement (requires registration): https://qdr.syr.edu/deposit/specialdeposit

XIII. Data discovery and identification

R13. The repository enables users to discover the data and refer to them in a persistent way through proper citation.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Response:

Making data findable, accessible, interoperable and reusable (FAIR, Wilkinson 2016) is a core mission of a data repository and QDR constantly seeks to improve the discoverability of its holdings. The Dataverse catalog used by QDR offers search, including powerful advanced search options as well as faceted browsing. Over the next year, QDR will be working towards extending the search capabilities to the file level, including full text and variable level (for tabular data) searches.

QDR's Dataverse catalog also provides harvesting facilities via OAI-PMH as well as a dedicated API, allowing machine-readable access to metadata. Currently, QDR metadata are harvested by Harvard Dataverse as part of the Data-PASS catalog. QDR also optimizes its metadata for the Datacite metadata kernel, which makes it accessible via the

DataCite Metadata store as well as the SHARE platform run by the Open Science Framework. Using JSON-LD/schema.org metadata embedded on item pages, QDR data are also findable through the newly released google dataset search.

As a member of the Data Citation Implementation Pilot group, QDR provides standardized citations as well as bibliographic metadata for reference managers, including Dublin Core and JSON-LD/schema.org metadata embedded on the page, for every project and every file. Every data project is registered with a DOI with DataCite and DOIs at the file level are planned this year.

Links:

QDR data findable through the Harvard Dataverse: https://dataverse.harvard.edu/dataverse/qdr

QDR data on OSF share:

https://share.osf.io/discover?publishers[]=Qualitative%20Data%20Repository&q=Qualitative%20data%20repository

Google dataset search: https://toolbox.google.com/datasetsearch/search?query=10.5064

Wilkinson 2016: https://doi.org/10.1038/sdata.2016.18

XIV. Data reuse

R14. The repository enables reuse of the data over time, ensuring that appropriate metadata are available to support the understanding and use of the data.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Comments:
4 – The guideline has been fully implemented in the repository

Response:

QDR encourages re-use of data in its repository by displaying it with rich context and by actively promoting it via social media and other channels. If the archiving of qualitative data is a very new endeavor for social scientists who engage in qualitative research, re-using qualitative data collected or generated by another scholars is even more unfamiliar. As such, QDR is developing a research agenda on the reuse of qualitative data and continuously seeks to adapt its practices to facilitate reuse.

Documentation and metadata are crucial pre-requisites for the the reuse of data by third parties. For metadata, QDR only strictly enforces minimal, Dublin Core requirements on data (title, author, description, subject, deposit date). However, as part of the curation process QDR typically develops significantly richer metadata in collaboration with the depositors. QDR's metadata profile is based on the Data Documentation Initiative (DDI) version 2.5 (Codebook), in line with most other social science data repositories. The repository is actively monitoring developments of the DDI standard that would provide better support for qualitative data, but the current "Lifecycle" (3.2) version of the standard holds little advantages for qualitative data. In particular, the use of DDI 2.5 is in line with other repositories with significant qualitative data holdings such as the UK Data Archive. As an XML format, DDI can be converted to updated forms of the standard using XSLT.

DDI output is currently automatically generated by the Dataverse software QDR uses. There is significant interest among the Dataverse user and development community to further improve DDI support (including a DDI-Dataverse working group of which QDR is a member), so that further developments of the DDI are likely to be incorporated into Dataverse.

QDR ensures the understandability of all deposited data through intensive, manual curation by its subject experts. QDR curators read all documentation and regularly request changes or additions to improve understandability. They also work with depositors on structuring their deposit and naming data files to maximize the ability of others to understand and ultimately re-use the data. The approach to curation is documented in the curation policy.

The licenses used by QDR allow for re-use of all data in research and teaching, but generally disallow the re-publication of data elsewhere, i.e. data are not under open licenses. The license terms are specified in QDR's Standard/special download agreements. These less permissive licenses are chosen due to the complex nature of some qualitative data, e.g., those under copyright, which limits their sharing, and those gathered from human participant, which can only be shared in a way such that research participants remain protected. QDR's practices are based on the practices and recommendations of comparable repositories such as the UK Data Archive. The repository will consider publishing data under open CC-BY-SA (Creative Commons Attribution Share-Alike) or CC0 (Public domain waiver) licenses and is moving towards publishing all documentation under a CC-BY-SA license.

Links:
Curation policy: https://qdr.syr.edu/policies/curation

Metadata application profile: https://qdr.syr.edu/policies/metadata

Standard deposit agreement (requires registration): https://qdr.syr.edu/deposit/standarddeposit

Special deposit agreement (requires registration): https://qdr.syr.edu/deposit/specialdeposit

DDI-Dataverse working group:
https://ddi-alliance.atlassian.net/wiki/spaces/DDI4/pages/70391592/DDI+Workflows+for+Dataverse

TECHNOLOGY

XV. Technical infrastructure

R15. The repository functions on well-supported operating systems and other core infrastructural software and is using hardware and software technologies appropriate to the services it provides to its Designated Community.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Response:

QDR follows ISO 14721:2012 , section 4.1.1.1 (common services) as a reference model for technical infrastructure development. The technical directors for QDR, in consultation with a Technical Advisory Board, monitor the implementation of services, and review emerging standards for qualitative data management on a biannual basis.

Infrastructure development activities follow an annual roadmap produced by QDR's technical directors, and approved by the QDR's Technical Advisory Board.

Hardware and software inventories and configuration information are recorded in a QDR managed wiki, and updated quarterly. All software running the production environment of QDR is open-source - this includes operating systems running on EC2 and S3 servers (Linux), a content management system based on Drupal, a repository framework based on Dataverse, as well as a suite of configuration management (Chef), continuous integration (Jenkins) and monitoring tools (Nagios). To further ensure continuous delivery of deployed code, our team also relies upon open-source tools to perform automated tests (Selenium) as well as infrastructure execution and management tool (Terraform). Each of these tools are well-supported by open-source communities. Our technical directors, and system administrator regularly monitor security and vulnerabilities related to this suite of software.

The hardware used to run QDR is provisioned at Amazon Web Services, and managed by our technical development team. Our infrastructure at AWS is configured with a set of Virtual Private Clouds for security (described in detail in R16), and we ensure proper bandwidth is available by using Elastic Load Balancing which distributes incoming user traffic across multiple EC2 instances.

Links:
ISO 14721: https://www.iso.org/standard/57284.html
Terraform: https://www.terraform.io/
Nagios: https://www.nagios.org/
Chef: https://www.chef.io/solutions/infrastructure-automation/
Selenium: http://www.seleniumhq.org/
Dataverse: http://dataverse.org
Security and infrastructure: https://qdr.syr.edu/policies/security
Digital preservation policy: https://qdr.syr.edu/policies/digitalpreservation

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

XVI. Security

R16. The technical infrastructure of the repository provides for protection of the facility and its data, products, services, and users.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Response:

Security and risk management are carried out by QDR's technical team, in collaboration with the Syracuse Maxwell School IT department, and a contract with a cloud infrastructure provider AWS. Dedicated instances purchased from AWS include brand new "10xlarge" servers (10x is a proprietary distinction by Amazon that indicates a dedicated server running on Intel Haswell processors) - that are refreshed every two years. Technical infrastructure is physically located in US-EAST (Ohio), but can be moved relatively quickly through QDR's use of the infrastructure management tool Terraform (as described in R15). QDR created a virtual private cloud (VPC) for different applications deployed to AWS. The VPC is achieved through private IP subnets, as well as a virtual private network (VPN) that secures access to the VPC (this is achieved through authentication).

As described in R9 and R12, QDR creates redundant storage (located both at Syracuse and in the cloud with AWS) that prevents data loss, and limits the impact of service outages in the case of a natural disaster.

End-user access to data requires registration, and agreement to QDR's General Terms and Conditions of Use (described in R2).

Links:
Terms and conditions: https://qdr.syr.edu/termsandconditions
Security and infrastructure: https://qdr.syr.edu/policies/security

Reviewer 2

Comments:
Accept

APPLICANT FEEDBACK

Comments/feedback

These requirements are not seen as final, and we value your input to improve the core certification procedure. To this end, please leave any comments you wish to make on both the quality of the Catalogue and its relevance to your organization, as well as any other related thoughts.

Response:

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept