Standard Operating Procedure (SOP) for Use of the REDCap Platform

SOP Code: DDPH-REDCAP-SOP-01
Version: 1.3
Effective Date: [DD/ MM/YYYY
Review Date: [14/01/2026]
Approved Date: [DD/MM/YYYY]
Developed by dr Massimo Mirandola and dr Ruth Joanna Davis
Reviewed by dr. Angelo Mazzotta
Approved by prof. Aldo Scarpa / Director of Department

Table of Content

Dipartimento di Diagnostica e Sanità Pubblica
Piazzale Ludovico Antonio Scuro n.10 – 37134 Verona | T: +39 045 8027022-7604
Prof. Aldo Scarpa - Mail: aldo.scarpa@univr.it
P. IVA 01541040232 | C.F. 93009870234

1. Purpose

This SOP defines the roles, responsibilities, and procedures governing the use of the REDCap platform at the Department of Diagnostics and Public Health (DDPH), University of Verona, ensuring secure, ethical, and compliant data management.

2. Scope

This SOP applies to all REDCap projects hosted by DDPH and all users involved in data collection, management, and analysis.

3. Definitions, roles and responsibility

REDCap: Research Electronic Data Capture (REDCap) is a secure, web-based software platform designed to support the creation and management of databases and online surveys for academic and scientific research. It provides audit trails, user-level access controls, and data export functionalities, supporting compliance with data protection and research governance requirements.

Electronic Case Report Form (eCRF): An electronic Case Report Form (eCRF) is a structured, electronic data-collection instrument implemented within the REDCap platform, designed to capture study-specific data as defined in the approved study protocol. The eCRF supports standardised data entry, validation, and quality control, and enables the collection of anonymised or pseudonymised data in compliance with applicable ethical, regulatory, and data protection requirements.

REDCap Administrator: The REDCap Administrator is responsible for the technical management and maintenance of the REDCap infrastructure. Responsibilities include activating projects in draft mode to enable eCRF development by Principal Investigators, moving projects to production mode upon verification of ethics approval (when applicable), managing user accounts and ensuring the secure operation of the system. REDCap Administrators operate in accordance with institutional policies and data protection requirements and do not access study data unless strictly necessary for system maintenance or technical support.

Project Users: Project Users are authorised individuals who access and use the REDCap platform in accordance with this SOP and the approved study protocol. They are responsible for ensuring data confidentiality, safeguarding system security credentials, and processing data in compliance with applicable ethical, legal, and data protection requirements, including Regulation (EU) 2016/679. They have specific roles assigned described below.

Dipartimento di Diagnostica e Sanità Pubblica
Piazzale Ludovico Antonio Scuro n.10 – 37134 Verona | T: +39 045 8027022-7604
Prof. Aldo Scarpa - Mail: aldo.scarpa@univr.it
P. IVA 01541040232 | C.F. 93009870234

Principal Investigator (PI): The Principal Investigator is the individual legally responsible for the project and all data with overall responsibility for the scientific, ethical, and regulatory conduct of the research project. The PI is accountable for the appropriate use of the REDCap platform, the authorisation and supervision of project users, and compliance with applicable ethical, legal, and institutional requirements.

Co–Principal Investigator (co-PI): The Co–Principal Investigator supports the Principal Investigator in the scientific and operational conduct of the project and acts under the PI's authority. The co-PI is authorised to access, enter, edit, validate, and export pseudonymised research data within REDCap and to manage user access as delegated, in compliance with the approved protocol and applicable data protection requirements. The co-PI does not hold primary legal responsibility for the project.

Investigator (I): An Investigator is authorised to access, enter, and edit pseudonymised study data within REDCap, execute data validation rules, and generate study-related reports. Investigators operate strictly within the scope of the approved protocol and the principle of data minimisation, without permissions for user management or unrestricted data export.

Data Clerk (DC): A Data Clerk is authorised solely for the entry of pseudonymised study data into REDCap, based on source documents made available by authorised personnel. This role does not include permissions for data editing, validation, reporting, data export, or user management, in line with the principle of least privilege.

Data Monitor (DM): A Data Monitor is authorised to review pseudonymised study data for data quality, completeness, and protocol compliance. The DM may execute validation rules and generate monitoring reports but does not have permissions for data entry, data editing, data export, or user management.

Data Analyst: A Data Analyst is authorised to access, and export pseudonymised datasets from REDCap exclusively for statistical analysis and reporting purposes, in accordance with the approved Statistical Analysis Plan and the principle of purpose limitation. This role does not include permissions for data entry, data editing, or user management.

Ethics Review Board (ERB): The Ethics Review Board is the competent independent body responsible for reviewing, approving, and monitoring research projects involving human participants, ensuring that they comply with ethical principles, applicable legislation, and institutional policies.

Dipartimento di Diagnostica e Sanità Pubblica
Piazzale Ludovico Antonio Scuro n.10 – 37134 Verona | T: +39 045 8027022-7604
Prof. Aldo Scarpa - Mail: aldo.scarpa@univr.it
P. IVA 01541040232 | C.F. 93009870234

User Privileges: User privileges define the specific permissions and access rights assigned to an individual user within the REDCap platform. Privileges determine which functions a user is authorised to perform (data entry, data editing, data validation, reporting, data export, user management, project configuration, and API access). User privileges are assigned on a role-based and principle-of-least-privilege basis, ensuring that each user is granted only the minimum level of access necessary to perform their authorised tasks in accordance with the approved study protocol, institutional policies, and applicable data protection legislation.
Privileges within a project are assigned by the Principal Investigator. All privilege assignments, changes, and revocations must be documented, traceable and auditable. Users are personally responsible for the appropriate use of their assigned privileges and must not attempt to access functions, data, or system resources beyond their authorised level of access. Any misuse, unauthorised privilege escalation, or inappropriate access may result in suspension or revocation of access and may trigger institutional disciplinary procedures. User privileges must be reviewed periodically and updated promptly in the event of role changes, project closure, or termination of affiliation, to ensure ongoing compliance with security, governance, and data protection requirements. This is a responsibility of the Project PI. The Principal Investigator (PI) shall conduct a periodic review (at least every six months) of the system logs (Audit Trail) to verify the legitimacy of access and promptly detect any unauthorized access attempts or anomalous data processing activities.

Anonymous data: Anonymous data are data that do not relate to an identified or identifiable natural person, meaning that identification of the data subject is not possible, either directly or indirectly, by any means reasonably likely to be used. Once data are effectively anonymised, they fall outside the scope of Regulation (EU) 2016/679 (GDPR), as re-identification is no longer possible.

Pseudonymised data: Pseudonymised data are personal data in which direct identifiers have been replaced with a code or pseudonym, while the additional information necessary to re-identify the data subject (re-identification key) is kept separately and securely, with access restricted to authorised personnel. Pseudonymisation reduces the risk of identification but does not eliminate it; therefore, pseudonymised data remain personal data and are subject to the provisions of Regulation (EU) 2016/679.

Application Programming Interface (API): The REDCap Application Programming Interface (API) is a programmatic interface that enables authorised systems or scripts to securely access, extract, and exchange data with the REDCap platform using authentication tokens. The API allows automated data retrieval, integration with external systems, and batch operations that may not be achievable through the standard web interface. API access introduces additional information security, data protection, and governance risks.

Dipartimento di Diagnostica e Sanità Pubblica
Piazzale Ludovico Antonio Scuro n.10 – 37134 Verona | T: +39 045 8027022-7604
Prof. Aldo Scarpa - Mail: aldo.scarpa@univr.it
P. IVA 01541040232 | C.F. 93009870234

Data Breach Notification and Escalation: Any actual or suspected personal data breach involving REDCap projects—including but not limited to unauthorised access, data loss, accidental disclosure, or compromise of credentials—must be reported without undue delay to the Principal Investigator and the institutional Data Protection Officer (DPO). The Principal Investigator, or any other authorised actor who becomes aware of the breach, is responsible for ensuring that the DPO is formally notified within 24–48 hours of becoming aware of the incident. This timeframe is necessary to allow appropriate assessment, mitigation measures, and, where required, notification to the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali) within 72 hours, in accordance with Regulation (EU) 2016/679 (GDPR). All data breaches must be documented, including their nature, scope, potential impact, and remedial actions taken, regardless of whether notification to the supervisory authority is ultimately required.

4. Procedures

Access to the REDCap platform is granted exclusively for academic and scientific research projects formally linked to the institutional activities of the Department of Diagnostics and Public Health (DDPH). Projects requiring ethical approval may be moved to production mode only after receipt of final approval from the competent Ethics Review Board.

Only anonymous or pseudonymised data may be entered into the system, and all data processing activities must comply with the General Data Protection Regulation (EU) 2016/679 and applicable data protection legislation. Once a project is in production mode, structural changes must be carefully managed, as modifications may result in data loss or compromise data integrity.

User access must be actively maintained throughout the project lifecycle, and any individual who ceases to collaborate on the study must be promptly removed from the REDCap project to ensure data security and regulatory compliance. Activation of the project and assignment of roles and responsibilities require completion of a specific form attached to this SOP (Terms and conditions for the use of the REDCap platform of the Department and Delegation Log for Authorisation to Use the REDCap Platform)

5. API Roles, Responsibilities and Restrictions

API Authorisation: API access may only be enabled upon explicit authorisation by the Principal Investigator and communicated to the REDCap Administrator, and only when justified by a documented scientific, operational, or technical need consistent with the approved protocol and data protection assessment (where applicable).

Dipartimento di Diagnostica e Sanità Pubblica
Piazzale Ludovico Antonio Scuro n.10 – 37134 Verona | T: +39 045 8027022-7604
Prof. Aldo Scarpa - Mail: aldo.scarpa@univr.it
P. IVA 01541040232 | C.F. 93009870234

API Token Responsibility: API tokens are personal, confidential credentials and must be protected with the same level of security as user authentication credentials. API tokens must not be shared, embedded in publicly accessible code repositories, or transmitted via insecure channels. The user to whom the API token is issued remains fully responsible for all activities performed using that token.

Permitted Use: API access shall be limited to the minimum data and functions strictly necessary for the approved purpose (principle of data minimisation and least privilege). API-based data extraction must comply with the approved protocol, Statistical Analysis Plan, and applicable data protection requirements.

Logging and Traceability: All API activity is subject to system logging and audit where technically supported. Users must ensure that local scripts and external systems maintain adequate traceability, version control, and access controls.

Data Protection and Security: Data retrieved via the API must be stored, processed, and transmitted in compliance with Regulation (EU) 2016/679 and institutional security policies. Local storage environments used for API-driven data processing must implement appropriate technical and organisational safeguards (e.g., encryption, access controls, secure backups).

Third-Party Systems and Integrations: Connection of REDCap via API to external platforms, cloud services, or third-party software requires prior assessment and authorisation to ensure GDPR compliance, data localisation requirements, and contractual safeguards.

Revocation and Incident Management: API access may be suspended or revoked at any time in case of misuse, security incidents, protocol deviation, or non-compliance. Any suspected or actual data breach, credential compromise, or abnormal API activity must be reported immediately to the REDCap Administrator and the institutional Data Protection Officer, in accordance with incident response procedures.

Liability: Users granted API access remain personally accountable for compliance with this SOP, institutional policies, and applicable legislation. Misuse or negligent handling of API credentials or extracted data may result in legal consequences.

6. Data Ownership Outside DDPH

If data ownership lies outside DDPH, a data processing agreement must be signed prior to data entry.

Dipartimento di Diagnostica e Sanità Pubblica
Piazzale Ludovico Antonio Scuro n.10 – 37134 Verona | T: +39 045 8027022-7604
Prof. Aldo Scarpa - Mail: aldo.scarpa@univr.it
P. IVA 01541040232 | C.F. 93009870234

7. Project status

Project in Development Mode: A project in development mode is a REDCap project that is under design and testing and not yet authorised for live data collection. In this phase, investigators may create and modify data collection instruments, test branching logic, validate calculated fields, and simulate data entry using test records.

Project in Production Mode: A project in production mode is a REDCap project that has been formally authorised for live data collection involving real study participants. Transition to production mode is permitted only after receipt of final ERB approval, where required. Once in production mode, the project serves as the official research database for the study, and all data must be managed in accordance with the approved protocol, consent documentation, and applicable regulations.

8. Transition from Development to Production Mode.

The transition of a REDCap project from development mode to production mode represents a critical step in the project lifecycle and is subject to the following conditions:

Must be requested by the Principal Investigator: The transition must be formally initiated by the Principal Investigator using the ad hoc REDCap procedure available at the end of the project set-up menu. This ensures that the PI confirms the readiness of the project for live data collection and accepts responsibility for the accuracy and completeness of the project structure.

Requires submission of final ERB approval (if applicable): For projects involving human participants and requiring ethical review, final approval from the competent Ethics Review Board must be obtained before the project can be moved to production mode. Documentation of the approval must be provided to the REDCap administrators as evidence of authorisation to begin data collection.

Is performed by the REDCap administrators: The actual transition to production mode is carried out exclusively by the REDCap administrators. This centralised process ensures that institutional governance requirements are met and that the transition is properly documented.

Marks the formal start of authorised data collection: Once the project is moved to production mode, the collection of real participant data is formally authorised. From this point onwards, data entered in REDCap are considered official study data and must be managed in accordance with the approved protocol, ethical approval, and applicable data protection regulations.

Dipartimento di Diagnostica e Sanità Pubblica
Piazzale Ludovico Antonio Scuro n.10 – 37134 Verona | T: +39 045 8027022-7604
Prof. Aldo Scarpa - Mail: aldo.scarpa@univr.it
P. IVA 01541040232 | C.F. 93009870234

9. Project Closure

Upon completion of data collection, REDCap projects must transition from data collection to data cleaning and analysis. During this phase, data entry should be locked or restricted as appropriate, and user access reviewed to ensure that only authorised personnel involved in data cleaning and analysis retain access. No further data collection should take place once the project enters this stage.

Once data cleaning and analysis activities have been completed, and no further access to the database is required, the project must be formally marked as "Completed" within the REDCap system. Marking a project as completed renders it inaccessible for data entry or modification and removes it from users' active project lists. Completed projects can only be viewed via the "Show Completed Projects" option and are no longer available for routine use.

Project completion marks the end of authorised database use. At this stage, the Principal Investigator remains responsible for ensuring that data are archived, retained, or deleted in accordance with the approved study protocol, applicable data protection legislation, and institutional policies. Where required, the REDCap administrators must be contacted to support project archiving or permanent deletion.

10. Compliance

Non-compliance may result in suspension of REDCap access.

11. Annex

Annex 1: Terms and conditions for the use of the REDCap platform of the Department and Delegation Log for Authorisation to Use the REDCap Platform.

Dipartimento di Diagnostica e Sanità Pubblica
Piazzale Ludovico Antonio Scuro n.10 – 37134 Verona | T: +39 045 8027022-7604
Prof. Aldo Scarpa - Mail: aldo.scarpa@univr.it
P. IVA 01541040232 | C.F. 93009870234

Annex 1

Terms and conditions for the use of the REDCap platform of the Department and Delegation Log for Authorisation to Use the REDCap Platform

The undersigned Prof./Dr. _____, employed at the Operative Unit of _____, within the Department of Diagnostics and Public Health of the University of Verona, in the capacity of Principal Investigator of the study (title and/or acronym):

REQUESTS (tick one or more boxes)

the creation of a personal account to use REDCap of the Department of Diagnostics and Public Health of the University of Verona; access credentials will be sent only to institutional e-mail address. ☐

the creation of a new project in REDCap of the Department of Diagnostics and Public Health of the University of Verona (a blank project will be activated and configured according to the study) (to be requested for each new project). ☐

the creation of REDCap Department of Diagnostics and Public Health of the University of Verona accounts for the following collaborators: ☐

Name	Surname	Institution e-mail	Role*	Exp. date dd/mm/yyyy

Dipartimento di Diagnostica e Sanità Pubblica
Piazzale Ludovico Antonio Scuro n.10 – 37134 Verona | T: +39 045 8027022-7604
Prof. Aldo Scarpa - Mail: aldo.scarpa@univr.it
P. IVA 01541040232 | C.F. 93009870234

***Roles:**

- **PI = Principal Investigator** (legaly responsible for the project and the data entered; full management of the project roles and data—entry, editing, export,—and of user roles with access to the project)
- **co-PI = co-Principal Investigator** (full management of the project roles and data—entry, projct editing, export—and of user roles with access to the project)
- **I = Investigator** (data entry and editing, execute validation rules and report creation)
- **DC = Data Clerk** (data entry with no exporting or editing data privileges)
- **DM = Data Monitor** (data check, execute validation rules and report creation)
- **Data Analyst:** Access, and export pseudonymised datasets for statistical analysis and reporting purposes.

By requesting access to the REDCap installation of the Department of Diagnostics and Public Health, University of Verona, and the set-up of a data-entry project, you acknowledge and agree to the following terms and conditions:

- This REDCap installation is provided exclusively for academic and scientific research purposes. Any commercial use or use for profit-making activities is strictly prohibited.
- Only projects formally linked to the institutional activities of the Department of Diagnostics and Public Health, University of Verona, are permitted.
- Projects requiring Ethics Committee approval will be moved to production mode only after receipt of final Ethics Review Board (ERB) approval. Official approval documentation must be sent to the REDCap administrators at redcapddph@ateneo.univr.it prior to activation.
- All data must be handled in full compliance with the General Data Protection Regulation (GDPR) (EU) 2016/679, as well as any applicable national or international data protection legislation.

Dipartimento di Diagnostica e Sanità Pubblica
Piazzale Ludovico Antonio Scuro n.10 – 37134 Verona | T: +39 045 8027022-7604
Prof. Aldo Scarpa - Mail: aldo.scarpa@univr.it
P. IVA 01541040232 | C.F. 93009870234

- The Principal Investigator is responsible for ensuring that all research activities conducted within REDCap comply with ethical, legal, and institutional requirements.
- All individuals authorised to access the REDCap installation must be adequately trained in REDCap project management and use, according to their assigned roles and responsibilities. The Principal Investigator is required to maintain an up-to-date record of the specific training provided to all authorized collaborators, certifying their understanding of the security procedures and confidentiality obligations related to the REDCap platform.
- All authorised users must take all reasonable measures to ensure the confidentiality, integrity, and security of the data and systems accessed through REDCap. Any suspected or actual data breach must be reported to the REDCap Administrator and the institutional Data Protection Officer immediately and no later than 24 hours after discovery, to ensure compliance with the legal notification obligations under Art. 33 of the GDPR.
- Only data specified in the approved study protocol may be collected and entered into REDCap. All data must be anonymised or pseudonymised in accordance with the GDPR and REDCap Operating Instructions; no directly identifiable personal data may be recorded.
- The collection of direct or indirect personal identifiers that could lead to the identification of study participants must be avoided.
- In cases where data ownership lies outside the Department of Diagnostics and Public Health, University of Verona, a data processing agreement must be signed before any data are entered into the system.
- Data stored in REDCap will be processed solely for the purposes for which they were collected, in accordance with legal requirements and the informed consent provided by study participants (when applicable).
- Data will be deleted when the purposes for which they were collected no longer apply.
- All project collaborators must be appropriately informed about data protection and data processing obligations and must act in compliance with applicable privacy legislation.
- REDCap access credentials are personal and non-transferable. In the event of suspected compromise, passwords must be changed immediately and the REDCap administrators informed at redcapddph@ateneo.univr.it.
- Any user who ceases to collaborate on the study will be promptly removed from the REDCap project.
- Data can be collected in production mode. Users acknowledge that making changes to a project may result in data loss.
- In the event that the employment relationship with the University of Verona or the affiliation with the Department of Diagnostics and Public Health is terminated, the REDCap administrators shall be notified without delay in order to delete the project or transfer

Dipartimento di Diagnostica e Sanità Pubblica
Piazzale Ludovico Antonio Scuro n.10 – 37134 Verona | T: +39 045 8027022-7604
Prof. Aldo Scarpa - Mail: aldo.scarpa@univr.it
P. IVA 01541040232 | C.F. 93009870234

responsibility to another Investigator, subject to the prior approval of the Director of the relevant Operative Unit.

- Upon completion of the project, the REDCap administrators must be contacted to archive or delete the project.

By signing below, you confirm that you have read, understood, and agree to comply with the above conditions. Failure to comply may result in suspension or revocation of your REDCap access.

Principal Investigator (name and surname) _____

(signature) _____

Date _____

For approval

Director of the Operative Unit (name and surname) _____

Signature_____

Date_____

Dipartimento di Diagnostica e Sanità Pubblica
Piazzale Ludovico Antonio Scuro n.10 – 37134 Verona | T: +39 045 8027022-7604
Prof. Aldo Scarpa - Mail: aldo.scarpa@univr.it
P. IVA 01541040232 | C.F. 93009870234

Dipartimento di Diagnostica e Sanità Pubblica
Piazzale Ludovico Antonio Scuro n.10 – 37134 Verona | T: +39 045 8027022-7604
Prof. Aldo Scarpa - Mail: aldo.scarpa@univr.it
P. IVA 01541040232 | C.F. 93009870234