ISARIC TECHNICAL AND ORGANISATIONAL MEASURES (TOMs)

The technical and organisational measures outlined in this document are implemented by [ISARIC](https://isaric.org), University of Oxford in accordance with Article 32 of the [UK General Data Protection Regulation (GDPR 2021)](https://www.legislation.gov.uk/eur/2016/679/contents). They are subject to regular revision to ensure a level of security appropriate to risk in relation to latest best practice.

# Processing of the personal data

## Access control

The following measures prevent unauthorised persons from gaining access to data processing systems where personal data are processed.

|  |  |  |
| --- | --- | --- |
| **System** | **Technical measures** | **Organisational measures** |
| **University of Oxford** | Access to systems hosted by the University of Oxford require Single Sign-On (SSO), strong passwords, and multi-factor authentication.  Session timeouts and automatic lockout on multiple failed logins. | User permissions managed by the University of Oxford’s Medical Sciences Division Information Technology Services (MSD-IT) - Security Policy available [here](https://www.medsci.ox.ac.uk/for-staff/resources/information-technology/department-facilities/service-descriptions/msd-it-services-security-policy).  Mandatory annual information security training for all users. |
| **REDCap Data Management System** | REDCAP DMS is a secure, web-based data capture tool compliant with the Federal Information Security Act (FISMA) standards.  Technical controls have been penetration tested. Full description of all technical controls is available in the [REDCAP Technical Overview](https://projectredcap.org/wp-content/resources/REDCapTechnicalOverview.pdf) document.  REDCap passwords must meet University of Oxford MSD-IT [Security Policy](C://Users/kwitt/Downloads/MSD_IT_Security_Policy.pdf) standards.  Firewall controls prevent unauthorised access to the University of Oxford network and resources.  Encrypted connections via Transport Layer Security (TLS) 1.2.  Account lockout after predefined failed login attempts and session inactivity logouts. Audit trail capturing all user access and data activities. | MSD-IT hosting on a dedicated server with operational controls aligned to industry standards including ISO/IEC 27001. Server equipment is locked and accessible only by controlled, logged access.  Administrator accounts limited to a minimum number and require accreditation.  Access controlled via REDCap Data Access Groups (DAGs) by authorised administrators.All external users must be authorised by an institution that has executed a Terms of Submission with ISARIC.  See [REDCap General Security Overview](https://www.iths.org/wp-content/uploads/About-REDCap-Vanderbilt.pdf) for details of systems compliance with the Health Insurance Portability and Accountability Act (HIPAA) Part-11 and the UK General Data Protection Regulation (GDPR). |
| **Amazon Web Services** | Approved AWS infrastructure hosting Elastic Compute Cloud (EC2) and Simple Storage Service (S3) services under University of Oxford Information Security oversight.  Use of AWS Identity and Access Management roles and policies for granular access control.  Data encrypted at rest using AWS managed keys (SSE-S3).  Data transfers use secure protocols (HTTPS) with end-to-end encryption.  Access to AWS management console is through University of Oxford SSO with multi-factor authentication | AWS operates as a sub-processor under contractual obligation to comply with GDPR.  Servers are in the United Kingdom.  Compliance certified to ISO27001, ISO27017, ISO27018, and the CISPE Code of Conduct.  Regular audits and monitoring by University of Oxford Information Security team. Incident handling coordinated with AWS and University security offices. |

## Management Responsibility

Management of the ISARIC Data Platform is the responsibility of the ISARIC Data Team, under the direction of the Head of Data and the Executive Director. The team processes and enables access to data according to the instructions of the Data Controller defined in the Terms of Submission.

* Data Controller: The Partner Institution contributing data is the Data Controller. The Controller signs the ISARIC Terms of Submission and is responsible for defining and for securing all necessary approvals for the processing undertaken by ISARIC.
* Data Processor: The University of Oxford, on behalf of ISARIC, is the Data Processor. The responsibilities of the Processor are outlined in the Terms of Submission executed between the Controller and Processor.
* Data Ownership: Data entered on the platform is owned by the Data Controllers. Data can be removed from the platform upon request of the Controller.

## Authorisation control

Measures to ensure that authorised users can access data in accordance with their authorisation level and that personal data cannot be read, modified or removed without authorisation during processing.

|  |  |  |
| --- | --- | --- |
| System | Technical measures | Organisational measures |
| **University of Oxford** | Role-based access control enforced at operating system and application levels.  Detailed logging of all access. | User roles assigned based on least privilege principle.  Access rights strictly limited and regularly reviewed. |
| **REDCap Data Management System** | Role-specific permissions enforced to control data entry, editing, and extraction.  Automated audit trails log user activities for traceability.  All user actions timestamped and associated with user IDs. | Data Administrators trained and vetted prior to account assignment.  Access rights promptly revoked upon role change or termination.  Oversight by ISARIC Data Security Model committee ensuring adherence to data access policies. |
| **Amazon Web Services** | Implementation of fine-grained access permissions using AWS Identity and Access Management, restricting access to minimum necessary.  Continuous monitoring of access logs via AWS CloudTrail with alerts configured for unusual access patterns. | Contractual agreements enforce strict control over personnel authorised to access AWS data.  Incident escalation protocol is in place by the University of Oxford Information Compliance Team for suspected unauthorised access. |

## Pseudonymisation

To secure the privacy of data subjects, ISARIC accepts only pseudonymised data. Each Partner Institution that contributes data signs the ISARIC Terms of Submission that includes standard data clauses requiring the institution to make reasonable efforts not to transfer, disclose or otherwise make available any data that can lead to the identification of an individual. Data schemas used in ISARIC’s REDCap DMS do not include direct identifiers, structurally preventing the inclusion of such information. Data stored on AWS are mapped to the ISARIC data schema which is constructed to omit the capture of any directly identifying information. Mapping software and oversight are designed to identify and exclude any direct identifiers.

# Ensuring ongoing confidentiality integrity, availability and resilience of processing systems and services

## Transfer control

Measures implemented by ISARIC to ensure that personal data cannot be read, copied, altered or removed by unauthorised persons during transfer or while being stored, and that it is possible to verify and establish to which recipients’ personal data are intended to be transferred.

|  |  |  |
| --- | --- | --- |
| System | Technical measures | Organisational measures |
| **University of Oxford** | Registration of all university hardware and regular updates of antiviral software.  Encryption of all data in transit using TLS 1.2 or higher. | Data are transferred to known ISARIC research collaborators who sign contracts requiring them to comply with the same terms set out in the data controller’s terms of submission  Procedures for sharing data with ISARIC partners are regularly reviewed and updated. |
| **REDCap Data Management System** | Audit checks on data uploads to control security.  Encryption of all data in transit using TLS 1.2 or higher. | Regular review of de-identification procedures for data transfer.  Roles assigned for monitoring and managing data transfer security. |
| **Amazon Web Services** | Data are transferred using APIs, provided by AWS which enable files’ transfer over HTTPS and SFTP protocols with strong key exchange (RSA) and encryption (256 AES). APIs support secure data transfers with transport encryption and granular access controls. | Designated role of Data and Research Manager within ISARIC, responsible for data transfer monitoring, control and incident response. |

## Input control

Measures are in place to ensure traceability and control over all data input, changes and deletions.

|  |  |  |
| --- | --- | --- |
| System | Technical measures | Organisational measures |
| **University of Oxford** | All data transfers use s secure transfer protocols. These include REDCap’s *Send-It* function, Microsoft Teams secure file exchange, secure APIs, or equivalent systems that employ encryption in transit (TLS/SSL) and require authenticated user access.. | Regular audits of data entry processes.  Assignment of responsibility for data input monitoring to ISARIC Data team roles.  Clear procedures for authorisation of data changes. |
| **REDCap Data Management System** | Built-in audit trail capturing all user data activities.  Unauthorised changes prevented by role-based permissions.  Automatic logging of all data operations. | Guidance provided for data controllers on secure data entry processes.  Data entry rights periodically reviewed and revoked if redundant.  Compliance monitored by ISARIC Data Team. |
| **Amazon Web Services** | Application layer logging of data manipulations.  Restricted database and data storage (S3) user permissions limiting data input capability | User permissions restricted to ISARIC staff.  Designated role of Data and Research Manager within ISARIC, responsible for data transfer monitoring, control and incident response.  Incident response triggered upon detection of improper data changes and managed by University of Oxford Information Compliance Team. |

## Data request control

To ensure that personal data processed on behalf of the controller are processed in accordance with the controller’s instructions, processing is restricted to activities approved by the Data Controller in the signed Terms of Submission. Data controllers are the decision-making authority in the governance process for data access. All data sub-processors have agreements in place to secure compliance with the Terms of Submission and data protection regulations. A list of all approved sub-processors is available to download on ISARIC’s website at <https://github.com/ISARICResearch/CCP/raw/refs/heads/main/Analyses/Partner_Analyses_metadata.xlsx>.

# Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

## Availability & Recoverability control

Measures taken by ISARIC and the University of Oxford to ensure that personal data is protected against accidental destruction or loss (including data backups, secure storage of data, virus protection, mirroring etc.) and can be rapidly restored in the event of a physical or technical incident.

|  |  |  |
| --- | --- | --- |
| System | Technical measures | Organisational measures |
| **University of Oxford** | Mirror copies of data on the REDCap DMS are stored in two active primary data centres. All devices used on MSD IT systems have dual redundant power supplies. All servers and switches are connected to Uninterruptible Power Supply (UPS) to protect against electric outage. Data storage devices connect to the MSD ITS server systems which are also physically located in the same Data Centres.  The file store is made available over the MSD IT networked file system, which allows rapid recovery from server or other connectivity failures.  Daily incremental backups and weekly full backups stored on secure offsite servers.  Disaster recovery tested periodically. | Responsibility for restore operations assigned to MSD IT Services.  Formal disaster recovery and business continuity plans in place. Standard operating procedures in place and regularly reviewed for archiving, update of backup and restoration. |
| **REDCap Data Management System** | Data are stored on the University of Oxford systems. Back-up and recovery systems as described above including redundant data centre sites within failover support and routine testing of restoration capabilities.  Built-in audit trail captures all user activities. Unauthorised changes prevented by role-based permissions. | Data entry rights periodically reviewed and revoked if redundant.  Compliance monitored by ISARIC Data team.  Documented procedures for incident handling for data loss.  Regular staff training on backup and recovery protocols. |
| **Amazon Web Services** | Application layer logging of data manipulations.  Use of AWS multi-AZ replication for high availability.  Automated snapshot creation for EC2 instances and S3 versioning enabled.  Defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO). | Restricted database user permissions limiting data manipulation capability to the ISARIC data team.  Designated role of Data Manager within ISARIC, responsible for data transfer monitoring, control and incident response.  Incident response triggered upon detection of improper data changes.  AWS disaster recovery plans reviewed by University of Oxford Information Security.  Continuous monitoring of system health and automated failover. |

# Processes for regular testing, assessment and evaluation of the effectiveness of technical and organisational measures for ensuring the security of data processing

## Data protection management

Steps taken by ISARIC on behalf of University of Oxford for the ongoing active management of data protection.

|  |  |  |
| --- | --- | --- |
| System | Technical measures | Organisational measures |
| **University of Oxford & REDCap Data Management System** | Configuration management to enforce security baselines.  Continuous monitoring tools for security event detection.  Annual penetration testing and vulnerability assessments. | University of Oxford Information Security Office provides guidance, policies and compliance support, aligned to industry standards such as ISO/IEC 27001.  Designated ISARIC Data team regularly reviews the TOMS and monitors data protection measures with support from Oxford Information Security, Information Governance and Information Compliance.  Annual Security and Data Protection Awareness Training mandatory for all ISARIC staff. |
| **Amazon Web Services** | External and internal audits to maintain ISO 27001 and other certifications where applicable.  Automated scanning for vulnerabilities in cloud workloads.  Logging and alerting on security incidents via AWS Security Hub and CloudTrail. |  |

## Incident response management

ISARIC operates in compliance with University of Oxford-supervised organisational controls for reporting of personal data breaches to the UK Commissioner’s Office. Procedures include event logging, investigation and mitigation of vulnerabilities, notification and tracking. University of Oxford registration with UK Information Commissioner’s Office: Z575783X