IDDO TECHNICAL AND ORGANISATIONAL MEASURES (TOMs)

The technical and organisational measures presented in this document are implemented by IDDO in accordance with Article 32 GDPR (EU General Data Protection Regulation). They are continuously improved by IDDO to ensure a level of security appropriate to risk in relation to latest best practice.

1. Pseudonymisation and encryption of personal data

Access control

The measures below prevent unauthorised persons from gaining access to data processing systems with which personal data are processed.

Technical measures	**Organisational measures**
Login with University of Oxford single sign-on, strong password and multi-factor authentication.	User permissions management controlled by the University of Oxford's Medical Science Division (MSD IT).
Data is uploaded by contributors through a secure connection that is authenticated and encrypted using Transport Layer Security (TLS 1.2 as recommended by the National Cyber Security Centre) to securely move the data from the Contributor to the upload server within the Oxford secure network.	Individual user profiles for IDDO data processing systems to log and monitor access to data.
Once at rest the data is encrypted using a hybrid cryptography approach, combining symmetric and asymmetric key algorithms. Both the data and its method of decryption are securely encrypted and transferred to the High Compliance Server (HCS).	The High Compliance Server (HCS) is only available to a very select group of users on the Oxford network or via VPN managed by University of Oxford IT Services. Access is limited to users using a virtual desktop, thus restricting movements of files on and off the HCS.
Data contributions are securely deleted from the upload server and cleared from memory. This uses a command line programme that overwrites, truncates and renames file contents before unlinking from a directory, and uses 35 passes to overwrite data.	Once a unique identifier has been assigned for each record, the file can then be reviewed by IDDO to identify and remove protected health identifiers in accordance with HIPAA best practices. An audit trail is kept of the identifiers removed.

Authorisation control

Measures to ensure that those authorised to use data processing systems can only access the data subject to their access authorisation and that personal data cannot be read, modified or removed without authorisation during processing.

Technical measures	Organisational measures
Logging of access to data processing applications when entering, changing, and deleting data.	Minimum number of administrators.
All server activity is logged as it occurs and recorded on a logging server.	Management of user rights by administrators.
The Platforms employ a series of access controls based on ISO 27001 requirements for safeguarding data being processed and securing resources. These can be broken down into three broad categories: • **Physical and Environmental Controls:** Access to the building is controlled via a secure entry system and only authorised staff with a swipe card can enter the building and office space. • **Network controls:** Firewall controls are in place to prevent unauthorised access to Oxford University network and resources. • **User Access Management:** Servers are only accessible by approved system administrators who are registered and have been issued logon credentials. These are accessed via remote desktop and/or VPN. Desktop terminals and University network resources are accessed by approved users who have been issued with a University network username and password.	All server and web applications are subject to access controls, and users require login details to utilise the tools. Password ageing and quality controls are in place to ensure university passwords are of adequate strength and are reset at least every 180 days (as per guidance produced by the UK's National Cyber Security Centre).

Pseudonymisation

IDDO receives pseudonymised data from its Data Contributors and these data are then subjected to further minimisation through a de-identification process prior to any transfer to Third Parties (as defined within the Terms of Data Submission). See 'IDDO Data De-

identification Procedure' for a full description of technical and organisational measures related to this process.

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

Transfer control

Measures implemented by IDDO 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.

Technical measures	Organisational measures
IDDO data transfer standard operating procedure in place.	Regular review of IDDO data transfer processes.
Data transfer via encrypted connections such as HTTPS and TLS.	Regular review of de-identification procedures for transfer of data.
Transmission of pseudonymised data following de-identification procedure.	Designated roles within IDDO responsible for data transfer monitoring, control and incident response.

Input control

Measures at IDDO that ensure it is possible to check and establish retrospectively by whom personal data has been entered into, modified or removed from data processing systems.

Technical measures	Organisational measures
Secure Contributor Data Upload Environment hosted by the University of Oxford logging all data contributions linked to signed IDDO Terms of Data Submission.	Regular review of data pipeline processes to optimise data management and security.
Standardised logging of the entry, modification and deletion of data during processing to a secure database.	Data entry, modification and deletion traceable to individual authorised users.
To access de-identified data for further curation activities an Oxford desktop terminal and web browser is used to	Clear process for assignment of rights for data entry, modification and deletion.

connect to a web application on the demo server. Access to the server is restricted (username and password required) and only authorised users can access the application. The connection is secured by a HTTPS connection with TLS authentication, using a strong key exchange (RSA) and strong cipher (256 AES).	

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

Availability control

Measures taken by University of Oxford and IDDO to ensure that personal data is protected against accidental destruction or loss (including data backups, secure storage of data, virus protection, mirroring etc.)

Technical measures	**Organisational measures**
Backing filestores are deployed over redundant disk arrays in a RAID configuration which offers good protection against multiple disk failures.	Following any loss of service, no matter how it is caused, when the Server hardware and the communications infrastructure have been restored to the state they were in before the loss of service, the University of Oxford IT Services support team will ensure that the Server filestore is restored to at least the state it was in at the time of the last successful backup.
Servers are imaged daily allowing for the fast recovery of the complete server system. Server filestores are also be backed up to the University central backup service.	
The frequency and retention of backups is as follows: • Daily database backups are taken and kept for a week • A monthly database backup is taken and kept indefinitely • Daily incremental backups of the server filestore are taken Monday to Friday and kept for a week.	

• Full tape backups of the filestore taken once a month and kept indefinitely, to provide a historical archive and speed up filestore recovery if there has been complete loss of filestore.	
The HCS supports automatic virus scanning when files are decrypted.	

Recoverability control

Measures in place at the University of Oxford and IDDO capable of rapidly restoring the availability of and access to personal data in the event of a physical or technical incident.

Technical measures	Organisational measures
The Platforms are hosted on a virtual datacentre, provisioned through the Oxford University Private Cloud. The infrastructure is designed to be resilient to failure at multiple levels and is spread across sites to mitigate against a complete single site failure. The service is mirrored across two sites (Banbury Road and South Parks Road in Oxford, UK), with part of the service delivered from each site and data at each site replicated to the other. All components in the cloud are redundant, up to the sites themselves. In the event of failure, all data is secure (replication is asynchronous to within the last minute) and in the case of a disaster, or service disruption, it can failover to the alternative environment.	The University of Oxford Private Cloud team will evaluate the nature and duration of any failure. In the event of a complete site failure, workloads running on the failed site will be brought up on the other site and all services will be offered from one site for the duration of the site failure. Following any loss of service, no matter how it is caused, when the Server hardware and the communications infrastructure have been restored to the state they were in before the loss of service, the support team will ensure that the Server file store is restored to at least the state it was in at the time of the last successful backup.

4. 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 the University of Oxford and IDDO for the ongoing active management of data protection.

Technical measures	Organisational measures
Review of TOMs conducted annually with appropriate updates.	IDDO Data Governance focal point identified to monitor and control data protection measures, with support from the Senior Information Governance Officer, Nuffield Department of Medicine.
Documentation of all data protection regulations with access for staff.	University of Oxford Information Security Office provides guidance, policy and compliance support, aligned to industry standards such as ISO/IEC 27001.
Formalised data governance process for assessing requests for individual patient data in place, overseen by independent Data Access Committee managed by TDR/WHO.	Security and Data Protection Awareness Training mandatory for all staff to complete annually.
No more personal data is collected than is necessary for the respective purpose.	Data Protection Impact Assessment (DPIA) is carried out as required with oversight from the University of Oxford Information Compliance Team.
	University of Oxford registration with UK Information Commissioner's Office: Z575783X.

Incident response management

Support for security breach response and data breach process at the University of Oxford and IDDO.

Technical measures	Organisational measures
IDDO data breach standard operating procedures in place.	Documented process for detecting and reporting security incidents or data breaches with support from University of Oxford Information Security Office (also with regard to reporting obligation to supervisory authority).
	If an incident such as a data breach, virus/malware attack, data or physical asset loss for example are discovered the following procedure is followed: • On discovery incident reported immediately to IDDO Senior Management. • Compromised systems are isolated and contained.

	• Security incidents are logged and reported through the incident portal: https://infosec.ox.ac.uk/report-incident • The incident will be investigated by the University and IDDO OxCERT to ensure vulnerabilities are fixed and/or mitigated. • Notifications will be provided to all relevant stakeholders of impact, progress, fix/mitigation/resolution actions, along with any other pertinent information relating to the incident. • Incident, action and outcome is logged by IDDO and can be provided on request as part of annual reporting cycle.

Data request control

Measures to ensure that personal data processed on behalf of the controller can only be processed in accordance with the controller's instructions.

Technical measures	Organisational measures
All processing completed in accordance with the IDDO Terms of Data Submission signed by the Controller with the University of Oxford.	Obligation to comply with data protection regulations for all data sub-processors through signed agreement with the University of Oxford.
Formalised data governance process for assessing requests for individual patient data in place, overseen by independent Data Access Committee managed by TDR/WHO.	Obligation to comply with data protection regulations for all third-party Data Recipients through signed Data Use Agreement with the University of Oxford.
Data transfer following full governance approval and signature of legally-binding Data Use Agreement reflecting the terms of data use agreed by the Controller.	Prior review of the security measures taken by the sub-processor and their documentation by the University of Oxford Information Security Office.
Monitoring of remote access by approved third parties.	Mandating destruction of data for Data Recipients after termination of the agreement (two-year term as indicated in IDDO Data Use Agreements).
Monitoring of sub-processors listed in accordance with the IDDO Terms of Data Submission.	In the case of longer collaborations: ongoing review of the sub-processor and its level of protection as deemed

	appropriate by the University of Oxford Information Security Office.