STANDARD OPERATING PROCEDURE (SOP)

TITLE: DATA PROTECTION POLICY

DO NOT USE THIS SOP WITHOUT FIRST CHECKING IT IS THE LATEST VERSION

Document ID:	SOP-CR001
Version No:	1.0
Effective Date:	January 2020
Review Date:	N/A
Applicable Clinique Research Site(s):	All

Approved By:	Roseanne Onyia Founder/Director, Clinical Operations; Clinique Research
Signature:	
Date:	January 2020

1. PURPOSE:

The purpose of this SOP is to describe the procedure of data protection undertaken at Clinique Research and to ensure:

- All relevant parties (sponsors and sites) are consulted and can support the project.
- The proposed trials are a strategic fit and aligns with Clinique Research's core values.
- Research projects have the best possible outcome in terms of recruitment, patient safety, budget, and time frames.
- Identifiable information collected as part of any research project is recorded, handled and stored in a way that meets the requirements of the General Data Protection Regulation (GDPR).

2. SCOPE:

All clinical trials to be monitored and managed at Clinique Research.

3. APPLICABILITY:

This applies to all Clinique Research employees, contract staff and to all relevant external persons or parties proposing to engage in the clinical trial services at Clinique Research.

4. GLOSSARY OF TERMS:

Please refer to Clinique Research SOP Glossary of Terms (see Related Documents).

5. PROCEDURE:

The overall process is to ensure that access to identifiable personal data are restricted to only personnel who are authorized to see it.

Data protection in relation to data collection must be considered during protocol development. Only data that is necessary and required by the approved research project protocol should be collected and the requirement for directly identifiable data versus pseudo anonymized data should be justified. The protocol should describe how data will be handled and include information about the data to be collected and the method(s) of collection and who will have access to the data.

5.1 Data Collection

When data are pseudo anonymized, one master list with the identifier/codes and the participants' details will be kept separately from research data in order to link the participants' research data and medical health records. For multicenter studies, there may be several lists, one kept at each site to identify that site's participants. Such lists should be kept in locked cabinets away from the Investigator Site File (ISF) in suitably secure environments or in an electronic format as password-protected files saved on a secure network. No copies should be made. It is not always possible to anonymize data (e.g., consent forms, qualitative research) but the collection, storage and access to such data must be justified.

5.2 Data Storage

All data received in an identifiable form must be stored securely and separate from the project data and Case Report Forms (CRFs). Essential identifiable project documents kept as part of the Trial Master File (TMF) and ISF must be shredded. Files containing identifiable electronic data, including electronic data capture systems and electronic CRFs, must be password-protected and stored on a secure network. There may be instances where an encrypted memory stick could be used for short periods e.g., qualitative interview recordings. Identifiable electronic data should be stored separately from the main TMF with their location and access details recorded in the TMF.

5.3 Data Transfer

Identifiable data should never be sent through the regular postal service or using unencrypted email messages. The research project protocol will describe appropriate methods for data transfer. All data transfers should be approved by the Principal Investigator and must be logged and accompanied by a Data Transfer Form, signed by the staff member transferring the data and countersigned by the recipient. This can be in the form of an email trail. Passwords to unencrypt the data should be provided to the recipient separately from the data e.g., by telephone. All methods used for data transfer should be appropriately tested to ensure compatibility with the transfer process.

- By Post: All personal identifiable data sent or received by post, email or on electronic removable media should use only approved methods e.g., on encrypted memory cards, by registered post in tamper proof envelopes. All such deliveries should be logged as received along with the date of receipt and the name of the receiver. Documents containing sensitive personal data or audio/video recordings of consultations or interviews should be labelled with only the unique study identifier and sent by registered post or courier. The research project protocol will describe which postal methods should be used and advice sought from the Project Lead where necessary.

- By Email/Internet: Identifiable data must not be transferred using standard e-mail protocols. Secure File Transfers in the form of encryption, zipped password protected, or a secure file-sharing provider must be used. All such transfers should be logged as received along with the date of receipt and name of the receiver. The research project protocol will describe which methods should be followed and advice sought from the Project Lead where necessary.

5.4 Archiving and Destruction

Source documents, and trial-related electronic and other data must be stored safely and in accordance with the requirements of SOP for Archiving. At the end of the study, identifiable data must be disposed of in a confidential waste bag or shredded. The research contract and local policy on data destruction should be followed and advice sought from the Project Lead where necessary.

5.5 Confidentiality

Research team staff have a duty of confidentiality in relation to identifiable personal data. Any breaches of confidentiality by research team staff must be notified to Clinique Research by telephone or email.

5.6 Deceased Participants

Although GDPR relates only to living individuals, any research project data relating to deceased participants should be held, archived and destroyed in accordance with GDPR and this SOP.

6. VERSION CONTROL:

Document History	
Version	**Summary of Changes**
1.0	N/A – First Issue

7. APPENDIX:

Data Backup SOP
Clinique Privacy Policy
Clinique Information Security Policy