concluded between:

Foundation for Professional Development (Pty) Ltd

(Hereinafter referred to as "FPD" ("the Recipient")

(Registration number: 2000/002641/07)

and

[insert full legal name of person / institution]

("the Provider")

1. Introduction

1.1 The Provider intends to transfer the Data to the Recipient on the Transfer Date on the terms and conditions set out in this Agreement.

1.2 The purpose of this Agreement is to facilitate the lawful transfer of Project Data between the Parties, and to comply with the Protection of Personal Information Act, Act 4 of 2013 and Applicable Legislation by regulating the Processing of Data.

2. Parties

2.1 The Parties to this Agreement are:

2.1.1 **Foundation for Professional Development (Pty) Ltd**

(Hereinafter referred to as "FPD" / "the Recipient")

(Registration number: 2000/002641/07)]; and

2.1.2 [Insert the full legal name, registered address, and name of person signing this agreement in his/her own capacity or of the natural person who is duly authorised to represent the Party and sign this Agreement. **(Hereinafter referred to as "the Provider).**

3. Definitions and interpretation

3.1 In this Agreement, unless the context indicates otherwise, if a word starts with a capital letter it has the following meaning:

3.1.1 "**Agreement**" this data transfer agreement.

3.1.2 **"Applicable Legislation"** means any legislation applicable to the Processing of Data including, but not limited to the National Health Act, Act 61 of 2003, the Intellectual Property from Publicly Funded Research and Development Act, Act 51 of 2008, the Exchange Control Regulations in terms the Currency and Exchanges Act 9 of 1933, the Electronic Communications and Transactions Act 25 of 2002, the Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002, and the Cybercrimes Act 19 of 2020.

3.1.3 **"Appropriate Safeguards"** means the technical and organisational measures that a reasonable person would use to safeguard the Data as more fully set out in Annexure C.

3.1.4 "**Confidential Information**" means information relating to a Party's business and, without detracting from the generality thereof, includes information with regard to:

3.1.4.1 the Project's results, and/or intellectual and/or other proprietary interests;

3.1.4.2 a Party's trade secrets, including but not limited to its business and strategic plans, financial affairs, licensing agreements, contractual relations, business methods and know-how, technology, computer systems and other technical matters;

3.1.4.3 a Party's trade connections, including but not limited to the identity of, and its relations with, its customers or clients, financiers, suppliers and providers of services;

3.1.4.4 a Party's know-how relating to the manufacture, development, use or sale of any of its products, including its know-how with regard to its manufacturing techniques, prices, designs, specifications, formulae, systems, processes, materials and marketing; irrespective of the manner in which the information is disclosed, whether orally, visually or in computer language or by inspection or documentation or other objects; or the time when the information is or has been disclosed, whether before or after the Effective Date.

3.1.5 "**Data**" any information, electronic or otherwise, including Personal Information.

3.1.6 "**Data Breach**" a breach of security, negligently, intentionally or otherwise which leads to the access, destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information.

3.1.7 "**Effective Date**" Insert date

3.1.8 "**Expiry Date**" Insert date

3.1.9 "**Intellectual Property**" means any and all copyright, rights in inventions, patents, know-how, trade secrets, trademarks and trade names, service marks, design marks, design rights in get-up, database rights and rights in data, utility models, domain names and all similar rights and, in each case: whether registered or not; including any applications to protect or register such rights; including all renewals and extensions of such rights or applications; whether vested, contingent or future; and wherever existing.

3.1.10 "**Parties**" the parties to this Agreement; and "**Party**" means any one of them.

3.1.11 "**POPIA**" the Protection of Personal Information Act, Act 4 of 2013.

3.1.12 "**Processing Purpose**" the Recipient will Process the Data in terms of this Agreement, and for the purpose as set out in Annexure B.

3.1.13 "**Research Study** or **Project**" the Research Study or Project the Parties are involved in as set out in Annexure B.

3.1.14 "**Regulator**" the Information Regulator of South Africa as established by section 39 of POPIA.

3.1.15 "**Secure Data Transfer**" the transfer of Data using industry standard secure norms or as determined in this Agreement.

3.1.16 **"Signature Date**" the date of signature of this Agreement by the Party last signing in time.

3.1.17 "**Transfer Date**" the date the Data is transferred from the Provider to the Recipient

3.1.18 "**Term**" means the period of this Agreement as per **clause 5**.

3.1.19 **"Research Study** or **Project Data**" the Data to be transferred from the Provider to the Recipient as more fully set out in **Annexure A.**

3.2 For the purposes of this Agreement, the term **"Health Research"** shall have the meaning attributed to it in the National Health Act, Act 61 of 2003 and the term "Human Participant" shall have the meaning attributed to it in the Regulations to the National Health Act.

3.3 The terms **"Consent", "Data Subject", "Operator", "Personal Information"**, **"Processing", "Responsible Party"**, and **"Special Personal Information"** shall have the meanings attributed to them in POPIA.

3.4 Headings are for convenience and are not intended to be used to interpret the Agreement.

3.5 This Agreement must always be interpreted in a manner that is consistent with POPIA in order for the Parties to fulfil their obligations to comply with POPIA and Applicable Legislation.

3.6 The rule of construction that this Agreement will be interpreted against the Party responsible for its drafting or preparation will not apply.

3.7 The words "include", "includes", "including", "in particular" are used to set out examples and not to set out a finite list.

3.8 If the due date for performance of any obligation in terms of this Agreement is a day which is a non-Business Day then (unless otherwise stipulated) the due date for performance of the relevant obligation shall be the immediately preceding the Business Day.

3.9 Any reference in this Agreement to:

3.9.1 "**Business Hours**" shall be construed as being the hours between 08:00 and 16:30 on any Business Day. Any reference to time shall be based upon Central African Time;

3.9.2 a "**clause**" or "**schedule**" is a reference to a clause or schedule to this Agreement unless expressly stated otherwise;

3.9.3 "**Days**" shall be construed as calendar days unless qualified by the word "Business", in which case it shall exclude any Saturday, Sunday or Public Holiday;

3.9.4 "**Person**" means any natural or juristic person.

4. Scope and Purpose

4.1 This Agreement regulates the Data in relation to the Research Study or Project.

4.2 The Provider hereby undertakes to transfer the Data to the Recipient on the Transfer Date for the Processing Purpose via a Secure Data Transfer.

4.3 The Data may only be processed by the Recipient in terms of this Agreement, and on condition that the Recipient complies fully with POPIA where POPIA is applicable.

4.4 The primary purpose of this Agreement is to ensure that the Parties comply with POPIA and Applicable Legislation where appropriate, and to ensure that Appropriate Safeguards are taken in relation to the Data.

4.5 Nothing in this Agreement limits or excludes either Party's liability to Data Subjects or to the Regulator under this Agreement or POPIA.

5. Term and Termination

5.1 Notwithstanding the Signature Date of this Agreement, it shall come into full force and effect on the Effective Date and shall continue until the Expiry Date subject to clause 5.2 below.

5.2 At any time during the subsistence of this Agreement, either Party may terminate this Agreement for any reason whatsoever, on thirty (30) Business Days' written notice to the other Party.

6. Survival of provisions and consequences of termination

6.1 Clauses 3, 6, 7, 8, 11, 12, 13, 14, 17, 18, and 19 will survive the termination or expiry of this Agreement.

6.2 On termination or expiry of this Agreement, the Recipient agrees to return and/or delete all Data in its possession unless otherwise agreed on by the Parties.

7. Compliance with Health Research law

7.1 This Agreement shall be governed by, and construed and interpreted in accordance with the Laws of the Republic of South Africa.

7.2 If the Data contains Data that the Provider collected from Human Participants as part of Health Research, or that the Provider generated from bio-specimens collected from Human Participants as part of Health Research, irrespective of whether such Data falls within the ambit of POPIA, the Provider warrants that it complied with all the requirements of the National Health Act and the Regulations relating to Research with Human Participants, in particular that:

7.2.1 It obtained approval for such Health Research from a registered health research ethics committee; and

7.2.2 It consulted with community representatives, where deemed appropriate by such health research ethics committee.

8. Data Privacy Obligations on the Provider and Recipient

8.1 If the Data contains Personal Information, each Party warrants that:

8.1.1 The conditions set out in Chapter 3 of POPIA, and all the measures that give effect to such conditions, will be complied with fully.

8.1.2 Data Processing will always be conducted lawfully, in accordance with POPIA and Applicable Legislation, and in a reasonable manner that does not infringe on the privacy of the Data Subject.

8.1.3 If it is a South African public or private body it has registered its Information Officer with the Regulator.

8.1.4 Data will only be processed where, taking into account the purpose for which it is processed, the Processing is adequate, relevant and not excessive.

8.1.5 Data will only be processed where a ground of justification exists as set out in section 11 of POPIA.

8.2 If the Data contains Special Personal Information, the Parties warrant that, to the extent applicable, they will both comply with Part B, Processing of Special Personal Information contained in POPIA (sections 26–33).

8.3 If the Data contains Personal Information, the Provider warrants that:

8.3.1 All Data has been collected directly from a Data Subject, with Consent from the relevant individual Data Subject to Process the Data. Where any other lawful justification for collection other than Consent was relied upon for the original collection, the Provider shall record this in Annexure A as part of the Data.

8.3.2 The Data:

8.3.2.1 was collected for a specific, explicitly defined purpose;

8.3.2.2 will only be retained for as long as is necessary;

8.3.2.3 will only be Processed in a manner that is compatible with the purpose for which it was collected; and

8.3.2.4 will be transferred, stored and disposed of in compliance with POPIA and all Applicable Legislation.

8.3.3 Having regard to the purpose for which the Data was collected, reasonable steps will be taken to ensure that the Data is complete, accurate, not misleading, and updated where necessary.

8.3.4 Documentation of all Processing operations will be retained, and it will retain written records of its compliance with this Agreement.

8.3.5 All reasonably foreseeable risks to Data will be identified and documented, and Appropriate Safeguards will be established, maintained, and regularly audited and will form part of the mandatory discussions between the Parties' data protection officers in the regular meetings referred to in clause 20 below.

8.3.6 All reasonable requests made by the Regulator in relation to the Data will be complied with.

8.3.7 It has carried out reasonable checks on the Recipient's ability to comply with this Agreement, and that it will take steps to terminate this Agreement in the event that the Recipient is no longer able to comply with the Appropriate Safeguards and/or any part of POPIA.

8.3.8 It will co-operate with and notify the Recipient about requests and/or notices received from Data Subjects.

8.4 If the Data contains Personal Information, the Recipient warrants that:

8.4.1 It will only Process the Data for the Processing Purpose and only further process the Data in accordance with what has been expressly agreed by the Parties and in compliance with the Consent of the Data Subject and/or with section 15 of POPIA.

8.4.2 It will not transfer Data to any other person, save where required by law, or where in compliance with section 72 of POPIA, or where agreed by the Parties and in compliance with the Consent of the Data Subject and POPIA. In the event that Data is transferred to a jurisdiction where POPIA does not apply, the Recipient warrants that it will only transfer Data to a jurisdiction with adequate protection as set out in section 72(1)(a) of POPIA.

8.4.3 It will retain a written record of its compliance with this Agreement, including its Processing of the Data, and provide such written record if asked to do so by the Provider.

8.4.4 It will allow the Provider, on reasonable notice, to audit its compliance with this Agreement and with POPIA.

8.4.5 It will ensure that appropriate technical and organisational measures are taken, and that Adequate Safeguards will be taken in relation to the Data as set out in Annexure C.

9. Data Breaches

9.1 Where there are grounds to believe there has been a Data Breach, the Parties will, within 48 hours:

9.1.1 take reasonable steps to fix the breach;

9.1.2 ensure further steps are taken to stop the breach from continuing;

9.1.3 take action to prevent a breach from happening again; and

9.1.4 notify the other Party in writing about the Data Breach and steps taken in relation thereto.

9.2 Where the Data contains Personal Information, the Party which suffers the Data Breach will, within 48 hours:

9.2.1 notify the Regulator in writing;

9.2.2 comply fully with section 22 of POPIA; and

9.2.3 within 24 hours, convene a meeting of senior Party representatives to determine the reasonable steps to be taken, and to document compliance with this Agreement, POPIA, and other Applicable Legislation.

10. Data Subject Rights

10.1 Where the Data contains Personal Information, the Parties agree that they will facilitate Data Subject access rights, as provided for in sections 23 and 24 of POPIA.

10.2 Where the Data contains Personal Information, the Recipient confirms that should a Data Subject:

10.2.1 directly object to it about the Processing of their Personal Information; or

10.2.2 request it to confirm whether it holds Personal Information about them, the purpose of Processing such information, a record or description of the Personal Information held, or which third parties have or have had access to it; or

10.2.3 request the Recipient to rectify, correct or deletion their Personal Information, or cease Processing their Personal Information; or

10.2.4 seek to exercise any other rights the Data Subject may have;

10.2.5 the Recipient shall immediately and without undue delay forward such communication to the Provider, and collectively, the Parties shall within 5 (five) business days determine the appropriate steps to be taken.

11. Obligations of the Provider and the Recipient

11.1 The Provider gives no warranty that the Data:

11.1.1 has any particular characteristics or qualities; or

11.1.2 is fit for the purpose for which it is being transferred.

11.2 Both Parties agree that Appropriate Safeguards will be taken to protect the Data, and to ensure that the Data is not lost, damaged, or unlawfully accessed.

11.3 While both Parties undertake to do everything possible to ensure a positive outcome in relation to the Project generally, they cannot guarantee any specific result, and both Parties agree to participate in the transfer of the Data at their own risk.

11.4 In the event that either Party is no longer authorised to retain the Data or parts thereof, such Party will destroy all instances of the Data under its control and notify the other Party.

12. Licence to use Data

12.1 The Provider hereby grants to the Recipient a non-exclusive, non-transferable licence to use the Data for the Processing Purpose, for the duration of this Agreement, and the Recipient hereby accepts the grant of the licence on the terms and conditions contained in this Agreement.

12.2 The Recipient undertakes to ensure that only staff members, contractors, agents and/or relevant persons who are required as part of their function to access the Data will have access thereto, and that those employees will be fully conversant with the terms of this Agreement and the requirements of POPIA.

12.3 In the event that an unauthorised person(s) comes into possession of a copy of or gains access to the Data from the Recipient, the Recipient undertakes to comply with the steps listed in clause 9 above, and:

12.3.1 As soon as possible, and within 5 (five) days, take reasonable steps to retrieve the Data and all copies that the unauthorised person(s) might have made, and to take all further reasonable steps to prevent further unlawful distribution of the Data; and

12.3.2 Advise the Provider in writing of the steps taken in terms of 12.3.1.

13. Data Ownership

13.1 The Provider is and will remain the owner of the Data and all copies made thereof by the Recipient.

13.2 The Recipient may only make copies of the Data if required for purposes of the Research Study or Project.

13.3 Nothing in this Agreement shall be deemed to grant the Recipient ownership of the Data or ownership of any copies thereof.

13.4 The Data is transferred on a non-exclusive basis.

13.5 Notwithstanding clause 13.1 above, ownership of inferential data and meta-data arising out of the Data will vest with the Party that creates it.

13.6 If the Data, or the inferential data or meta-data contemplated in this clause are Personal Information, ownership in such Data is limited by the rights of Data Subjects in terms of POPIA.

14. Intellectual Property

14.1 Except as specifically provided for herein, each Party owns and retains all right, title and interest, worldwide, in any and all of its Intellectual Property pre-existing before the Effective Date of this Agreement.

14.2 All Intellectual Property developed as part of the Research Study or Project will be owned jointly by the Parties.

14.3 Regardless of a Party's location, to the extent applicable, both Parties warrant that they will comply with:

14.3.1 the Intellectual Property from Publicly Funded Research and Development Act, Act 51 of 2008; and

14.3.2 the Exchange Control Regulations in terms of the Currency and Exchanges Act, Act 9 of 1933.

15. Publication and Publicity

15.1 All communication between the Parties regarding the Research Study or Project and/or Data will be regarded as Confidential Information.

15.2 A Party will refrain from making public any results of the Research Study or Project:

15.2.1 unless that Party obtains the written consent of the other Party, or unless South African legislation provides otherwise; and

15.2.2 subject to compliance with the Intellectual Property from Publicly Funded Research and Development Act, Act 51 of 2008.

16. Benefit Sharing

16.1 The benefits that the Provider will receive from the Recipient in exchange for transferring the Data to the Recipient are described in Annexure D.

16.2 Apart from the benefits listed in Annexure D, all academic publications and press releases that report on the Research Study or Project must acknowledge that the Data were provided by the Provider.

16.3 If the Data are Personal Information, all academic publications and press releases that report on the Research Study or Project must:

16.3.1 ensure that no Data Subject is identified or identifiable from the publication unless the Data Subject's express Consent has been obtained for such publication;

16.3.2 take action to prevent discrimination, stigma or harm to any community identified in the publication; and

16.3.3 acknowledge the Data Subjects (anonymously) and where relevant the Data Subjects' community.

16.4 If the Data were generated from bio-specimens, either directly or indirectly, or are associated with bio-specimens, each Party warrants that it did not, and will not provide any reward in money or in kind to the Data Subjects, whether directly or indirectly, excluding health research ethics committee approved compensation for:

16.4.1 expenses incurred; and

16.4.2 time, inconvenience, and risk.

17. Indemnity and Limitation of Liability

17.1 Each Party indemnifies and holds harmless the other Party from all liability, losses, claims and expenses, including legal costs, arising from or connected with any unlawful conduct it is responsible for.

17.2 In no event will either Party be liable to the other for loss of profits, or for direct, indirect, incidental, special or consequential damages arising out of this Agreement.

18. Confidentiality

18.1 Each Party will keep confidential and will not, without the prior written consent of the other Parties, disclose to any person any Confidential Information of the other Party, including:

18.1.1 the details of this Agreement, the Data that will be processed, and the details of the negotiations leading to this Agreement; and

18.1.2 all information relating to the business and/or operations and affairs of the Parties which are not in the public domain.

18.2 The provisions of this clause shall not preclude any Party from making any disclosure:

18.2.1 to its professional advisors, provided that it will procure that such advisors comply with the provisions of this clause; and/or

18.2.2 which it is required to make by law.

19. Dispute Resolution and Arbitration

19.1 If any dispute, disagreement or claim of any nature arises between the Parties ("the Dispute") concerning the Data, the interpretation, execution, or implementation of this Agreement, or otherwise, the Parties shall negotiate in good faith to resolve the Dispute by negotiation between senior representatives of each Party.

19.2 Within a period of 14 days after the date on which the dispute arose (the Dispute Date) the Parties will meet to discuss the dispute and will endeavour to resolve the dispute amicably.

19.3 Each Party undertakes at such meeting to make full disclosure to the other of all information and records relating to the dispute.

19.4 The negotiation will entail that the Party claiming the Dispute must invite the other Party in writing to meet, either in person or via video conferencing (such as Zoom or Microsoft Teams or similar), and to attempt to resolve the Dispute within 10 (ten) days from date of the written invitation.

19.5 If the Parties are unable to resolve the dispute amicably within 10 days from the date of the written invitation, either Party may refer the dispute to FPD Managing Director or Chief Operating Officer and the Provider's Chief Executive Officer or their duly appointed representatives, who will use their best endeavours to resolve the dispute. Their determination will be final and binding and will be carried into effect by the Parties.

19.6 If the individuals described in 19.5 above fail to resolve the dispute within a period of 30 days after it has been referred to them, the Party claiming the Dispute may:

19.6.1 submit the Dispute to mediation to be administered by the Arbitration Foundation of Southern Africa ("**AFSA**"), in accordance with the rules of AFSA in relation to mediation, subject to 19.10 below;

19.6.2 failing agreement as aforesaid within 10 (ten) days of the Dispute being submitted to mediation, the Parties shall refer the Dispute for final resolution to arbitration in accordance with the rules of AFSA as provided for herein.

19.7 The arbitrator shall be legal practitioner of South Africa, with at least 15 (fifteen) years' post-admission experience in legal practice.

19.8 The arbitrator will be agreed upon between the Parties to the Dispute in writing. If the Parties are not able to agree upon the arbitrator within 10 (ten) days of the Dispute being submitted to arbitration, the arbitrator will be appointed by AFSA.

19.9 AFSA's Rules for Expedited Arbitration will be used.

19.10 Any mediation or arbitration will be held via video conferencing, unless the Parties agree otherwise.

19.11 The decision of the arbitrator will be final and binding on the Parties and may be made an order of court at the instance of any of the Parties to the Dispute.

19.12 Notwithstanding anything to the contrary in this Agreement, any Party will be entitled to apply for, and if successful, be granted, an interdict or other interim and/or urgent relief from the court.

19.13 The Parties irrevocably consent and submit to the exclusive jurisdiction of the North Gauteng High Court, Pretoria for relief.

20. Relationship Management

20.1 If indicated and appropriate both Parties will appoint a data protection officer for the purposes of ensuring compliance with this Agreement, and POPIA where applicable, and to generally manage the relationship between the Parties and the Processing of Data.

20.2 The data protection officers and any persons who the data protection officers may deem necessary will meet as often as may be necessary but no less than once every 3 (three) months, to consider the Processing of Data and general compliance with POPIA where appropriate, and to audit the Appropriate Safeguards to ensure they are maintained.

21. Force Majeure

21.1 No Party shall be liable for any failure to fulfil its obligations under this Agreement if and to the extent such failure is caused by any circumstances beyond its reasonable

control by a force majeure event, including: a pandemic, flood, fire, earthquake, war, hurricane, industrial action, government restrictions or acts of God, provided that any Party affected by such circumstances shall notify the other Party thereof as soon as is reasonably possible in the circumstances.

21.2 Should either Party be unable to fulfil a material part of its obligations under this Agreement for a period in excess of 30 (thirty) days due to circumstances beyond its control, as contemplated in this clause, the other party may, in its sole discretion, cancel this Agreement forthwith by written notice.

22. Notices

22.1 Any notice or other document whether for serving any court process or documents, giving any notice, or making any other communications of whatsoever nature and for any other purpose arising from this Agreement to be served under this agreement to a party shall be served at its address set out below:

22.1.1 Provider's notices:

email: [insert email address]

physical address: [insert physical address]

22.1.2 Recipient's notices:

e-mail: foundation@foundation.co.za

physical address: FPD Knowledge Park – East Block

173 Mary Street

The Willows

Pretoria

0184

22.2 All notices given in terms of this Agreement shall be in writing and any notice given by one party to the other which is sent by e-mail to the addressee's e-mail address shall be deemed to have been received by the addressee on the 1st (first) business day after the date of transmission thereof.

22.3 Notwithstanding anything to the contrary contained or implied in this Agreement, a written notice or communication actually received by one of the parties from the other

including by way of e-mail shall be adequate written notice or communication to such party.

23. General

23.1 This Agreement will in all respects be governed by and construed under the laws of the Republic of South Africa.

23.2 This Agreement does not establish any principal-agent or similar relationship between the Parties, and nothing in this Agreement shall be interpreted as allowing either Party to represent or act in the name or for the account of the other Party. The Parties shall act in all aspects as independent contractors.

23.3 This document constitutes the sole record of the agreement between the Parties in regard to the subject matter hereof.

23.4 No addition to, variation or consensual cancellation of this Agreement will be of any force or effect unless in writing and signed by or on behalf of all parties to this agreement.

23.5 No Party will be entitled to cede, assign or otherwise transfer all or any of its rights, interest or obligations under and in terms of this Agreement except with the prior written consent of the other Parties.

23.6 This Agreement may be executed in one or more counterparts, each of which shall be deemed to be an original, and all of which together shall constitute one and the same agreement.

23.7 The Parties agree to act with the utmost of good faith towards each other.

SIGNED at _____ on this the _____ day of _____ 202__

AS WITNESSES:

1. _____

2. _____

_____

PROVIDER

who warrants that he/she is duly authorised hereto

SIGNED at _____ on this the _____ day of _____ 202__

AS WITNESSES:

1. _____

2. _____

_____

RECIPIENT

who warrants that he/she is duly authorised hereto

Annexure A

Data to be transferred

In Annexure A, the Parties should include specific details about the Data being transferred. Each case will change according to its own facts, but the Parties must be as thorough and detailed as possible in describing the Data that is being transferred. In addition, where Special Personal Information is part of the Data, and this is collected without the Data Subject's consent, the Provider must record the lawful justification for the Processing of this Data in Annexure A.

The Provider will be the party that would populate this Annexure

Annexure B

Project and Processing Purpose

[insert]

Annexure B requires the Parties to include details about the research project and purpose of the Processing. Parties should comment on the context, scope, nature, and reasons for Processing.

Where the Data is transferred to FPD for purposes of the research undertaken by a student for example then FPD should set out why the data is needed. Once again the Provider should indicate what is needed from their side in this regard.

Annexure C

Technical and organisational measures to protect Data

Annexure C must be populated with information relating to the technical and organisational measures taken to protect the data. These measures are systems, procedures and controls that are in place – either physically (such as alarms or user access control) and in software and hardware. Details about what steps are taken to protect the Data should also be detailed in Annexure C. The technology in place, and software and/or hardware used to protect the Data should be set out. Also what software and/or other technical steps are in place to prevent data breaches? How and where is the data stored and what steps are taken to prevent unlawful access? In relation to organisational measures, specific processes and controls that are in place to ensure safety of Data should be mentioned. What are the systems and procedures used? Who has access to the data and/or server rooms? Is physical access secured with an alarm? What policies are in place?

Where FPD is the Recipient the Provider of Data should require FPD to comply with all the safeguards as mentioned above. If the Provider is FPD then FPD should insist that the Recipient provides the detail of how the Data will be protected.

For example where the student is working with a foreign University or organisation based in another country that student/ organisation should request FPD to provide detail on Data protection.

The Recipient's responsibilities will be to

- Ensure that all records, including electronic data sets, related to student research data provided to FPD by students are stored in line with data security, privacy and confidentiality requirements per Good Clinical Practices and FPD's policies and guidelines.
- Use FPD's infrastructure to manage all study-related documentation, datasets and resources. No information should be stored or kept outside of the designated FPD infrastructure.
- Ensure the data is stored on a Secure File Transfer Protocol (SFTP) site provided by Network Alliance and management by the FPD Monitoring and Evaluation (M&E) Unit. Once stored, the data is only accessible through the FPD Data Pipeline, which enforces user rights and

passwords. Only the FPD Managing Director and the Head of the FPD M&E Unit will have the required user rights and passwords. The server is firewalled with only the minimum required port open. A Virus scanner runs on the server.

Annexure D

[insert]

Annexure D should set out the benefits that the Provider will receive from the Recipient in exchange for transferring the Data to the Recipient. For example the student will be able to complete the research study and graduate if the Data is transferred to FPD. Where FPD is the Provider the situation will be according to the reasons why Data is transferred from FPD to a Recipient.