Imperial College
London

Airwave Health Monitoring Study Confidentiality Agreement

V3.1

All researchers working with Data collected by the Airwave Health Monitoring Study must read and, by their signature, agree to abide by the principles and specifics of this agreement in order to be granted access to Study Data. Data is any information relating to Study participants, whether stored electronically, in documentary form or imparted orally.

This agreement is additional to the College's Information Systems Security Policy, with which you should also be familiar and have accepted. In the event of any uncertainty on what is and is not permitted you should speak to your supervisor or the Study's Database Manager.

Exemptions to the conditions below are allowed when carrying out tasks specifically permitted by the Study's System Level Security Policy, or if you have been given a specific and personal exemption.

The following conditions apply to all persons working with Study Data:

1) You should read and understand "Personal Information in Medical Research", published by the Medical Research Council, which sets out your responsibilities to safeguard the confidentiality of all information to which you gain access in the course of your work, particularly that relating to identified individuals.

2) You must make no attempt to access any Data to which you have not been granted access, or facilitate such unauthorised access by others. You must not attempt to link your Data with any other data, whether derived from the Study or elsewhere.

3) You must not attempt to identify or make contact with any participant.

4) Printing Data containing personal identifiers is forbidden. Printing of anonymised person-level Data is discouraged; if you do, it must be stored securely and should not be removed from the College. When finished with, you must ensure all printed matter is securely shredded.

5) You must not publish, prepare or deliver a presentation (this includes teaching), or make reference in any electronic communication to Data relating to any individual participant or small group of participants.

6) You must ensure the Data is accessible only to authorised persons, which by default means you alone.

7) You will not use the Data after ceasing to be a member of Imperial College.

The following conditions apply to the use of participant-level Data, whether containing personal identifiers or not, on computers other than the Study's Private Network.

8) Data must be stored and processed only on the encrypted file system which will be prepared for you. You must not attempt to unencrypt the Data, make copies of it onto a non-encrypted file system, or make the encryption key available to an unauthorised person.

9) You must not make copies of the Data onto any device other than that agreed by the Database Manager (this includes backups), or remove any device or media containing the Data from your normal place of work.

10) You may access the Data remotely (i.e. from other than your normal place of work) only after prior agreement with the Database Manager. Any such agreement will normally require you to use the College's Remote Desktop Gateway, whose normal security features must be enabled. Remote Access should only be used on a device which you personally control, and never when you are in a public place.

11) You must ensure that all Data you have used is securely erased when you finished using it, and inform your supervisor or the Database Manager as appropriate.

Declaration

I understand the conditions set out above and will be personally responsible for safeguarding the confidentiality of all Data and information to which I gain access in the course of my work.

I am familiar with and am bound by the College's Information Systems Security Policy.

I will report any breach of this Agreement, or reasonable suspicion thereof, to the Database Manager at the earliest opportunity.

I understand that any breach of these conditions will be treated as a serious disciplinary matter.

PRINT NAME …… CID ……..

SIGNATURE ……

DATE ……