WOOLCOCK
LEADERS IN BREATHING & SLEEP RESEARCH

ABN 88 002 198 905

Woolcock Institute of Medical Research Limited

Digital Data Management Policy

Approved by the Board: 9 August 2017

1. Background

Woolcock Institute of Medical Research Limited (the Woolcock) understands it needs to control and protect any data it requires to meet its corporate and research objectives. For this purpose, data includes, inter alia, data that is acquired, developed, owned or deemed to be owned by the Woolcock.

The Woolcock's records and information are part of its corporate and research memory and represent a vital asset to support daily functions and operations.

They help the Woolcock to make good use of precedents and of organisational experience.

The Woolcock's records provide evidence of:

a) actions and decisions;
b) support policy formation, high level decision-making, business continuity, efficiency and productivity in research project delivery, management and administration;
c) protect the interests of the Woolcock, our employees, associates, patients and the community; and
d) help the Woolcock deliver its services and research in consistent and equitable ways.

2. Related policies

The Woolcock acknowledges this Digital Data Management Policy is interpreted and functions in association with the following Woolcock governance policies:

- Responsible Conduct of Research Policy – which sets out the conditions governing research practice in the Woolcock to comply with the Australian code for responsible research. In particular, it outlines how research data is to be controlled and managed;
- Intellectual Property (IP) Policy – which sets out who owns the IP developed within the Woolcock; and
- Privacy Policy – which sets out the Woolcock's obligations in meeting the Australian privacy principles.

3. Digital data management policy

These policy principles guide all data management procedures within the Woolcock.

1. The Woolcock or its affiliates own or is deemed to own all data.

2. Every data source must have a defined Custodian in a business / research leadership role, who has overall responsibility for the accuracy, integrity, and security of that data.

3. Wherever possible, data must be simple to enter, be clearly defined and accurately document its subject. Data must also be in a useful, usable form for both input and output.

4. Data should only be collected for a specific and documented purpose.

5. Data must be readily available to those with a legitimate business or research need.

6. Data capture, validation, and processing should be automated wherever possible.

7. Data must be entered only once whenever possible.

8. Processes that update a given data element must be standard across the information system.

9. Data must be recorded as accurately and completely as possible, by the most informed source, as close as possible to their point of creation, and in an electronic form at the earliest opportunity.

10. Data should be recorded and managed over time in an auditable and traceable manner.

11. The cost of data collection must be minimised.

12. Data must be protected from unauthorised access and modification.

13. Data must not be duplicated unless duplication is absolutely essential and has the approval of the relevant internal authority. The appropriate relevant internal authority will be determined at the time when the project / initiative governance structure is being created. In such cases, one source must be clearly identified as the master; there must be a robust process to keep all copies in step; and copies must not be modified (i.e., ensuring that the data in the source system is the same as that in other databases).

14. Data structures must be under strict change control, so that the various business and research system implications of any change can be properly managed.

15. Whenever possible, international, national, or industry standards for common data models must be adopted. When this is not possible, organisational standards must be developed, documented and implemented. These need to be approved by the Woolcock's Executive Management Committee.

16. Data should be defined consistently across the Woolcock where this principle can be applied. It is acknowledged that some research projects may not be able to comply with this requirement.

17. Users must accurately present the data in any use that is made of them.

4. Data breach

Should a data breach occur, the Woolcock will notify affected individuals and the Office of the Australian Information Commissioner (OAIC) of the data breaches that are likely to result in serious harm within 30 days of the breach event.

The factors which might contribute to a reasonable person thinking "serious harm" might have occurred include:

- The sensitivity of the information;
- Whether the information was encrypted;
- Whether the information was in a secure file;
- How likely it is that the security could be breached; or
- The identity of the person who obtained the information, whether they intend to cause harm to the affected person and the nature of the harm.

Policy review

This policy will be reviewed every two years.