School Population and Global Health

CONFIDENTIALITY OF RESEARCH DATA POLICY

The School of Population and Global Health (SPGH) policy on: Confidentiality of Research Data defines the scope, roles and responsibilities around the management of research data within the School.

PURPOSE

The Confidentiality of Research Data Policy (‘the Policy’) for the UWA SPGH has been developed to ensure that research data are handled appropriately and in accordance with the values and ethos of the Australian National Privacy Principles, the conditions under which the data have been made available and general community expectations.

The School acknowledges the importance and privilege of being granted access to personal health information for the purpose of research. As such, all personnel within or affiliated with the School have a responsibility to respect that privilege and to fulfil their legal and ethical responsibilities for maintaining the practice standards outlined in this Policy with regard to the access, storage, transport, handling and archiving/destruction of research data.

SUMMARY

This policy applies to all personnel and affiliates with the UWA SPGH who are making use of, or who could potentially come into contact with, research data of a confidential or personal nature.

This includes:
- full-time or part-time academic, general or IT staff;
- employees on casual contracts;
- adjunct appointments;
- external investigators who will be permitted access to School data;
- postgraduate researchers;
- undergraduate students; and
- work experience students.

General
- Upon commencement of work/study within SPGH, all personnel must:
  - agree to abide by the terms and conditions of the SPGH Confidentiality Policy; and
  - sign the School’s ‘Declaration of Confidentiality’ (APPENDIX A).
- Personnel are required to be familiar with the ‘identifiability’ categories of research data: identifiable; partially identifiable (coded/re-identifiable); non-identifiable (de-identified/anonymous).
Data Storage Requirements
• All research data must be collected and stored in accordance with this policy herein.
• Identifying personal information must not be stored with research data.
• Filing cabinets, computers and offices must be secure and be locked when not in direct use.
• All computers must be password protected with screen-lock activated.
• Data should be stored on the UWA Institutional Research Data Store (IRDS).
• Data on laptop/home computers and portable media (USB drives, external hard drives) must be encrypted or password protected and the hardware never left unattended unless stored securely.
• Undergraduate students are not permitted access to identifiable research data.
• Data must remain confidential and cannot be stored on a cloud-based system without approval from the data custodian.

Data Transmission
• Electronic data must be encrypted before transmitting via Cloudstor. Please read the section in relation to this carefully.
• Printing and faxing of data is not an acceptable practice.

Data file archiving and destruction
• On completion of the project, all electronic and hard copy records must be archived as per the Record Sentencing Process APPENDIX B (in an encrypted/password protected file or archive box marked ‘confidential), and forwarded to Academic Services for storage.
• When no longer required, archived data must be destroyed under the direction of the project’s current chief investigator or nominee.

Monitoring and governance
Any breach of this policy, whether intentional or unintentional, must be notified immediately to the Chair of the SPGH Research Committee. A review panel will be convened to consider any policy breach on a case-by-case basis, and sanctions may apply.

DEFINITIONS
Research Data
This term encompasses the many types of information relating to individuals participating in the conduct of research projects and includes:
• personal contact details;
• demographic data;
• clinical/medical information;
• occupational history;
• geocodes;
• general behavioural information; and
• various other types of personal information.

In addition, for the purposes of this Policy research data includes:
• written or recorded responses provided via interviews, focus groups, questionnaires, personal histories and biographies;
• information derived from human tissue (such as blood, bone, muscle and urine), including reports on genetic analysis of samples;
• material/information collected by audio, video or digital recording.
Categories of ‘Identifiability’ of Research Data

Personnel are required to be familiar with the ‘identifiability’ categories of research data:

**Identifiable**
Data that allow the identification of a specific individual are referred to as “identifiable data”. A person’s identity becomes ascertainable if there is reference to a single ‘unique’ identifier, such as unit medical record number (UMRN) that has negligible error in specificity (i.e. the identifier is unique to an individual person), or a combination of ‘partial’ identifiers that together achieve a similar level of ascertainability. Examples of partial identifiers include an individual’s name (noting that most full names are relatively unique in Australia), date of birth, occupational designation, residential address, telephone number, or other contact information.

**Potentially identifiable (coded, re-identifiable)**
Data may have identifiers removed and replaced by a code. In such cases it may be possible to use the code and a linkage key to re-identify the person to whom the data relate so that the process of de-identification is reversible. In these cases the data are referred to as “potentially identifiable”.

**Non-identifiable (de-identified, anonymous)**
The process of non-identification is irreversible if the identifiers have been removed permanently and the data have not been assigned a code to allow re-identification, or if the data have never been identified. These data are referred to as “non-identifiable”. However, it should be recognised that the term “non-identifiable” is used frequently, in documents other than this Policy, to refer to sets of data from which only names have been removed. Such data may therefore remain potentially “re-identifiable” if there is a linkage key that enables the data to be reassociated with personal identities at a later time.

**Encryption/Data Transmission**
This term refers to any process which translates data in a computer file into an unreadable form. Cloudstor (https://cloudstor.aarnet.edu.au supported by UWA) provides an encrypted link to download the data but doesn’t encrypt the data itself. You must first encrypt the data before uploading to Cloudstor - see https://www.veracrypt.fr/en/Documentation.html for reference.

**NOTE:**
- You must first obtain the approval of the data custodian before transferring any data via electronic means (i.e. USB, email etc.)
- Once you have been granted approval to transfer data, please contact UWA IT (IT-HMS@uwa.edu.au) if have any queries in relation to how to encrypt or send data.

DATA STORAGE REQUIREMENTS

**General Requirements**
- Upon commencement of work/study within SPGH, all personnel must agree to abide by the terms and conditions of the SPGH Confidentiality Policy; and sign the School’s ‘Declaration of Confidentiality’ (APPENDIX A).
- All research data, of any type (see above definitions) from any source (e.g. discrete research project, commissioned research program) should be collected and maintained in accordance with the Commonwealth Government Information Privacy Principles of the Privacy Act 1988 (https://www.oaic.gov.au/privacy-law/privacy-act/), as well as the Australian National Privacy Principles (https://www.oaic.gov.au/agencies-and-organisations/guides/australian-privacy-principles-
Any changes to the personnel working with research data obtained from the State or Commonwealth government, must first be approved by the WA Department of Health Human Research Ethics Committee (http://www.health.wa.gov.au/healthdata/HREC), UWA Human Research Ethics Committee (http://www.research.uwa.edu.au/staff/committees/hrec) and/or other relevant institutional ethics bodies. This requires completion of a project amendment form with details of the personnel changes (including addition of students to a project) which must be submitted to, and approved by, the relevant ethics body before personnel changes can take effect.

No State or Commonwealth individual unit record research data (of any type), where the UWA SPGH is the approved research organisation, should be forwarded to another institution or person, unless approval has been provided by the UWA Human Research Ethics Committee, the WA Department of Health and/or the Commonwealth data custodian.

Personal identifying information (e.g. names, address, contact details) should NOT be stored with confidential health/clinical records or other confidential data unless it is absolutely essential for the conduct of the project (e.g. personal identifiers should be stored in a separate computer, or directory, to the one containing the confidential health information where possible). Such information should be removed from confidential records when no longer required.

All office environments where data are to be stored must be secured with restricted access to non-authorised personnel. The requirements are as follows:
- Offices, filing cabinets and other storage facilities containing confidential research data should be locked when not in direct use.
- Office, desk and filing cabinet keys should not be provided or loaned to any non-authorised person, or left unattended at any time.
- Any keys that are misplaced must be reported immediately to Academic Services.

In instances where data are to be stored/analysed external to the UWA SPGH (e.g. such as working at home), due diligence is required to ensure appropriate security of research data, especially where shared computers are used. The specific steps/processes to ensure adequate security of electronic and hard copy research data are outlined below.

Where data are part of a collaborative, multi-institutional project between SPGH and other schools/universities/hospitals/government departments, data stored or analysed within SPGH is required to be maintained in accordance with this policy. In addition, data stored within other organisations should be maintained according to this policy except where the external organisation has their own data protection policy equivalent to that outlined here. Where the collaborating institution is also the data custodian (e.g. WA Department of Health, hospital, Raine Study), then that organisation/institution’s data protection policies will apply for data maintained within those locations.

**NOTE:** Data must remain confidential and cannot be stored on a cloud-based system without approval from the data custodian.

**Electronic Records**

- Login passwords are required for all computers (desktop and portable) containing identifiable, potentially identifiable or non-identifiable research data. Passwords must not be shared.
- When unattended, office computers should be shut down, or have the screen lock function enabled with password access required. The use of automated screen locking when computers have been idle for ≥10 minutes is recommended.
• Computer logon passwords for all hardware containing individual-level research data are to be changed every three months.

• Identifiable, potentially identifiable or non-identifiable data should be primarily stored on the Institutional Research Data Store (IRDS), where access is securely controlled. In instances where large data files may need to be stored on a local hard drive, the security measures outlined above should be implemented.

• Chief investigators responsible for research data stored on the Institutional Research Data Store (IRDS) have permission to add or remove personnel. Requests need to be lodged as outlined at http://www.library.uwa.edu.au/research/irdss

• Those wishing to use data offsite must have the prior approval of the Chief Investigator and receive confirmation from UWA IT (IT-HMS@uwa.edu.au) that their laptop or home computer complies with the required security criteria outlined.

• Research data stored on electronic systems external to the SPGH (including external storage devices, laptops and home computers) should be restricted to approved users only and maintained in a ‘secure’ environment in accordance with the institution/agencies guidelines/standards. Wherever possible, when not in use laptop computers and external electronic storage devices should be maintained in a locked cabinet when stored at home.

Those wishing to use data offsite must have prior approval of the data custodian and receive confirmation from UWA IT (IT-HMS@uwa.edu.au) that the device they wish to use (i.e. laptop or home computer) complies with the required security criteria outlined above.

The other specific requirements relating to data stored on laptops and home computers are as follows (NOTE – these criteria do not apply to all data approval and the investigator is responsible for ensuring compliance with restrictions for data on laptops etc):

  o Any health data stored on a laptop or home computer must be file-encrypted, or stored in an encrypted volume/folder if being used for current analysis, using encryption software approved by the UWA IT department. Further, access to the Windows environment must be through password login. A password of at least 8 characters must be used to access the encrypted folder on the laptop or home computer.

  o Where possible, it is recommended that laptops and computers used to store research data external to the School should be the property of University and not personally owned by the researcher.

  o At no point should laptops containing research data be left unattended (e.g. in cars, during travel, at the data collection site) or given to non-authorised personnel.

  o If external/portable data storage is required, such as data being entered in laptops during the data collection phase of a project or data stored/analysed external to the School (e.g. when working from home), such methodology must be stated in the project ethics application(s).

**NOTE:** Whatever decision is made by the data custodian as to the place of analysis (desktop at SPGH / laptop / home), this must have been clearly outlined in data and ethics applications and have been approved.

After completion of analysis for a research project, files containing identifiable, potentially identifiable or non-identifiable data should be removed from laptops or home computers, and stored within School
storage facilities only. To guard against deleted files being recovered, especially if the computer is sold or given to non-authorised personnel, data should be deleted using a secure deletion program (such as ‘Eraser’ which is freely downloadable from: http://eraser.heidi.ie/), a job should also be logged via the IT Service Desk (IT-HMS@uwa.edu.au) to request deletion of the profile and to verify the computer before deploying it to the next user.

- A research analyst who leaves the School before the completion of analysis must ordinarily deposit a copy of the research data with a member of the School staff approved by the analyst’s supervisor. After this, the research analyst must permanently delete all versions and copies of the data from any home or notebook computer in their possession that will not be returned to the School. This requirement may be modified with permission from the Head of School where a student has accrued intellectual property rights to the data or in other circumstances where there are appropriate reasons for the researcher to retain a copy of the data. In those instances, the conditions under which the data are to be managed must adhere to this Policy and be carefully documented and agreed between the School and research analyst in writing. If any IP issues exist, this should be reviewed by the UWA’s Office of Research Development and Innovation (RDI) and UWA Legal Services before data is removed from School premises.

Other types of storage for research data, such as portable media (e.g. external hard drives, USB drives etc) must be maintained securely when not in use, with no unauthorised access permitted. Authorisation from the supervisor is required prior to creating a portable media of the data and all such portable devices must be encrypted using Veraveracrypt which is approved by UWA’s IT department and can be freely available software that can be downloaded from https://archive.codeplex.com/?p=veracrypt/.

A copy of passwords for encrypted portable electronic data devices will be securely maintained by the Chief Investigator. As such, staff and students are required to inform the Chief Investigator of encryption passwords for all portable media devices used to store research data.

**Hard Copy (Paper) Records**

- Where possible only aggregated non-identifiable data should be produced in hard copy.
- Hard copy records containing confidential health or other personal data at the unit/individual level should only be maintained when absolutely essential for the conduct of the research. Where identifiable data are required to be produced in hard copy, such material should be maintained in a ‘restricted-access’ lockable cabinet, in a lockable office when not in direct use. Offices should be locked when unoccupied, with the exception that emergency procedures override this requirement.
- Storage facilities should be kept locked at all times when not in direct use. Only the research personnel identified in the approved ethics application(s) or who have signed confidentiality agreements related to the project should be permitted access to the data.
- Office keys and security keys must not be given or loaned to any non-authorised person. In addition, misplaced or lost keys must be reported immediately to Academic Services and at no time should security keys be copied without the permission of the relevant project chief investigator.
- In such cases where individual unit records containing identifying information are required in hard copy, data should be outputted wherever possible via a printer that is accessible only to the approved analyst(s). Printed data should be collected and securely stored immediately upon printing.
- When transporting hard copy patient identifiable information, data should be transported in a locked secure briefcase, secure document holder or similar. Such data should not be left unattended at any time during transportation.
Additional Requirements for Undergraduate Students

In accordance with existing School policy, undergraduate population health major or honours students are NOT permitted to access identifiable data from confidential clinical patient records (such as from medical notes in hospitals). This policy remains in place irrespective of any ethical approval that would otherwise allow access. It does not, however, pertain to data collected directly from consenting patients/study participants by the student nor to data specifically accessed for the purposes of undertaking duties directed by a student’s supervisor whilst on practicum placement.

Honours students are not permitted to hold individual level patient data for their project (identifiable, re-identifiable or non-identifiable) on non-School computers (i.e. home desktops or personal laptop computers). All analyses of such data must be undertaken either within the confines of SPGH using School provided hardware or within the confines of the workplace of the principal supervisor, for example at the Telethon Institute of Child Health Research, providing the same security measures as outlined in this policy are in place. For students enrolled in the Population Health major on practicum placement, analyses must occur within the confines of a computer at the hosting agency.

All individual level data used for undergraduate student projects must be de-identified either at the source or by the supervisor upon receipt prior to analysis by the student.

TRANSMISSION OF RESEARCH DATA

Mail

- Hard copy paper records containing identifying confidential clinical, personal or demographic information may be mailed, providing the research data are separated from patient or participant identifiers and mailed separately.

- Identifiable or potentially identifiable data stored on electronic media may be mailed, providing data are encrypted prior to copying to portable media. Alternatively, data may be secured using password-protected zip files, with de-encryption passwords sent separately or via alternative medium (e.g., by phone or email).

- Where possible, the use of official courier services for delivery of hard copy research data is recommended to permit tracking of materials and confirmation that research data were received by the intended recipient.

- The sender must confirm that the data has been received by the intended recipient. Follow-up with intended recipients should be undertaken by the sender if acknowledgement of receipt of data via mail is not received within four days.

Email

- Identified or potentially identifiable data must not be sent in the body of an email.

- Identifiable or potentially identifiable data must be encrypted, or secured using password-protected zip files, prior to being sent as an attachment to an email.

- Encrypted or zipped data files and de-encryption and/or zip passwords must be sent in separate email messages, separated by a period of at least 12 hours, or passwords may be communicated immediately by alternative medium (e.g. phone or fax).

- Emailed data (adhering to the process outlined above) must be sent to an email address that can only be accessed by the intended recipient or authorised personnel. Recipients should treat confidential data in accordance with the guidelines set out by this Policy.
• When emailing research data, the sender should request a ‘confirmation of receipt’ from the intended recipient. Follow-up with intended recipients should be undertaken by the sender if acknowledgement of receipt of data via email is not received within 48 hours.

ARCHIVING AND DESTRUCTION OF DATA FILES

• Upon completion of the project, the chief investigator(s) must ensure that all electronic and hard copy records are archived and stored securely for an appropriate length of time (usually 5-7 years after publication, or up to 25 years for paediatric research data), in accordance with the NHMRC Code for the Responsible Conduct of Research (Section 2.1, Responsibilities of Institutions for retention of research data and primary materials; 2.1.1: www.nhmrc.gov.au/publications/synopses/_files/r39.pdf), and the guidelines from UWA Archives and Records Management Services (www.archives.uwa.edu.au/).

• Electronic research data should be archived in a password-protected zip file, or in an encrypted file, and stored in either a folder on the School of Population & Global Health network or work desktop computer that can be accessed only by the approved researchers. Alternatively, archived electronic data can be stored, in the above-mentioned secured formats, on a CD/DVD/USB which is maintained in a restricted-access locked cabinet.

• Hard copy research data should be placed in an archive box marked as confidential with the chief investigator’s name, content, School Administration-allocated box number, date of packaging and date of destruction clearly indicated. Archive boxes should contain data from a single project only and be packed in accordance with UWA archiving guidelines. Archive boxes should then be forwarded to the Academic Services Team Leader for storage.

• When archived data is no longer required, all computer files and paper records must be destroyed under the direction of the project’s chief investigator. Paper records can be destroyed by shredding or placing in the School-provided locked security bin. Computer files should be deleted using security deletion software approved by UWA’s IT department (such as ‘Eraser’ which is freely downloadable software from: http://eraser.heidi.ie/). Optical media (CDs, DVDs, floppy disks and tapes) are to be manually destroyed using physical methods such as permanent watermarking of discs using IT approved equipment. For further information on archiving or the procedures for data destruction, contact the Academic Services Team Leader.

IT STAFF ACCESS TO ELECTRONIC CONFIDENTIAL RESEARCH DATA

As stated above, unless otherwise indicated, it is required that research data be placed on the UWA Institutional Research Data Store (IRDS) with access restricted to the approved analysts on each project. However, in order to perform regular backup of such data (both internally and to an offsite location), Faculty IT personnel will require periodic access to these files at the level required for whole-of-file operations.

At no time will IT personnel access the unit/individual record data containing health or medical information within these data files, given that this would be in breach of legal protections under which these data were supplied to the approved research personnel.

MONITORING, GOVERNANCE AND ADMINISTRATIVE SAFEGUARDS

• Supervisors of commencing staff and postgraduate students are required to ensure they accept the Terms and Conditions of the Policy and advise the UWA IT department the access to be granted to research data maintained on the UWA Institutional Research Data Store (IRDS).
• Heads of each research Centre/Group within the School are responsible for ensuring compliance of research personnel and activities within their remit, to the School Confidentiality of Research Data Policy. An annual monitoring process of policy compliance is to be implemented within each research Centre/Group in the School with confirmation of compliance provided in writing to the Chair of the School’s Research Committee on an annual basis.

• The School reserves the right to conduct periodic ‘spot checks’ of adherence to this policy by research groups with the School by the Research Committee.

• Periodic reminders regarding data security issues may be circulated by approved personnel as necessary.

• Any breach of this Policy, whether intentional or unintentional, and regardless of who committed the breach, must be notified immediately to the Chair of the SPGH Research Committee. A Review Panel, comprising the Head of School, Research Committee Chair and Academic Services Team Leader (or other senior staff member if any of these personnel are responsible for the breach), will be convened to consider each notified policy breach. Sanctions for breaches of this Policy do apply, ranging from compulsory re-education to employment contract termination, with consideration given for each breach of this Policy on a case-by-case basis according to the facts in each instance. Any penalty imposed will not override those implemented by the relevant data custodians.

POLICY REVIEW

The School Confidentiality of Research Data Policy will be reviewed on an annual basis by the School Research Committee, or earlier if the need arises.

RELATED POLICIES


Confidentiality and intellectual property - http://www.postgraduate.uwa.edu.au/students/policies/ip


SCHOOL OF POPULATION AND GLOBAL HEALTH

Acceptance of the Terms and Conditions as set out in the
Confidentiality of Research Data Policy

All staff (full time, part time, casual and adjunct), postgraduate students and visitors working on research data within the UWA School of Population & Global Health (SPGH) are required to familiarise themselves with the Confidentiality of Research Data Policy. Research team Heads and student supervisors should provide personnel under their supervision/management with a copy of the Policy and discuss this policy prior to staff completing the acceptance below.

<table>
<thead>
<tr>
<th>UWA SCHOOL OF POPULATION &amp; GLOBAL HEALTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIDENTIALITY OF RESEARCH DATA POLICY ACCEPTANCE</td>
</tr>
</tbody>
</table>

I have read the Confidentiality Policy and discussed it with my supervisor/manager. I accept the terms and conditions as stated in the policy:

Name: ___________________________  Staff/Student Number: __________________

Signature: ________________________  Date: __________________________

Team Head/Supervisor Name: ___________________________

Team Head/Supervisor Signature: ________________________  Date: __________________________