Summary of PRECRU Data Management Plan

PRECRU (Prehospital, Resuscitation and Emergency Care Research Unit)
Curtin School of Nursing
Curtin University, Kent St, Bentley 6102

This document last saved: 14 Apr 2023

PRECRU's Data Management Plan specifies the policies, procedures and technologies for PRECRU's management of patient data.This Data Management Plan was developed by Fifth Domain[1] (April 2016), and subsquently endorsed and implemented by PRECRU. Below is a summary of the Management Plan. Further details can be provided on request (judith.finn@curtin.edu.au).

1. PRECRU's Data Security Management Team oversees the policies, procedures and technologies relating to PRECRU's management of confidential patient data. This team consists of the PRECRU Data Security Manager, PRECRU Director, and respective deputy roles.

2. All confidential data stored by PRECRU are encrypted using FIPS 140-2 approved encryption algorithms (e.g. VeraCrypt[2] encryption software), and decrypted using volume-specific digital "key files". Access to key files is only via password-protected hardware-encyrpted USB flash drives[3] (one drive per PRECRU member). This system restricts access of each confidential dataset to specific PRECRU team members (i.e. even Curtin University IT staff are prevented from viewing these data in their decrypted form). In the event that a flash drive is lost or stolen, unauthorised access is prevented by the drive's requirement for keypad password entry (7-digit minimum password length, and automatic wiping of the contents after 10 consecutive failed password attempts).

3. In addition to protecting confidentiality through encryption, any confidential data stored by PRECRU on the Curtin University Network are stored on a restricted-access PRECRU folder, with access to sub-folders restricted to specific individuals, as authorised by the Director of PRECRU.

4. Physical transfer of confidential data into or out of PRECRU is via password-protected hardware-encrypted USB flash drives[4]. In the event that a flash drive is lost or stolen, unauthorised access is prevented by the requirement for keypad password entry (and 7-digit minimum password length, and automatic wiping of the contents after 10 consecutive failed password attempts).

5. Electronic transfer of confidential patient data to or from external locations (e.g. SJA-WA; WA Department of Health; WA Registry of Births, Deaths and Marriages; Monash University) is via secure connection (e.g. secure file transfer protocol; Virtual Private Network (VPN)). Any confidential patient data imported to (or exported from) PRECRU are imported directly into (or exported directly from) encrypted volumes. Where data are transferred via VPN between a PRECRU-controlled source to a PRECRU-controlled destination, both the source and destination are mounted as encyrpted volumes.

6. Electronic transfer of WA Health Department data also requires:
   Identifiers must be transmitted separately
   Transmission is via secure file transfer protocol
   Personal health information must not be transported overseas without the required approvals

7. PRECRU's Data Security Manager maintains a Data Security Asset and Access Register. The Asset Register records the user (or location) of each of PRECRU's physical Data Security Assets (e.g. USB flash drives). The Access Register records approved access to confidential datasets for individual PRECRU members.

8. Approval for data access is determined by the PRECRU Director and implemented by the PRECRU Data Security Manager. Data access is not granted until the requesting individual signs the relevant confidentiality agreement(s), agreeing to the conditions of data use.

9. PRECRU computers and other Data Security Assets (e.g. USB flash drives) must remain under the physical control of PRECRU staff and students. A heavy-duty physical safe is used for storage of PRECRU Data Security Assets that are not in use.

10. Any deletion of confidential data from computers, servers or external storage (e.g. hardware-encrypted USB flash drives) is done using Eraser[5] software. This software completely removes data from a computer/server/drive by overwriting it multiple times.

11. Confidential data may only be reported in de-identified (e.g. aggregated) format – so that no individual can be reasonably re-identified. Clinician collaborators who are invited to be co-authors on publications will not have access to any identifiable patient-level data.

12. If there is a need to print patient data, printing will only be on a local printer that is not connected to the corporate network. Paper records containing personal health information are archived in locked storage at Curtin University. Any disposal of printed patient data is via shredding/pulping at facilities approved by the Director of PRECRU.

13. Research data will be securely retained for a minimum of 7 years from the date of the last publication or end of the project, whichever comes later, for non-clinical studies and 25 years for clinical trials.

14. Data will be securely destroyed after the required retention period unless the Director of PRECRU mandates the data are to be retained. It is the Principal Investigator's responsibility to oversee data destruction, and to notify the data custodians when data is destroyed (and where required, notify the WA Health Department Human Research Ethics Committee, and WA Data Linkage Branch).

References

NHMRC *Australian Code for the Responsible Conduct of Research*:
https://www.nhmrc.gov.au/guidelines/publications/r39,

WA DoH Practice Code for the Use of Personal Health Information:
http://www.health.wa.gov.au/healthdata/docs/090429_Practice_code_for_the_use_of_personal_health_information.pdf

Curtin University's Research Data and Primary Materials Policy:
http://policies.curtin.edu.au/findapolicy/docs/Research_Data_and_Primary_Materials_Policy.pdf

Footnotes:

[1] Fifth Domain: https://www.fifthdomain.com.au/

[2] VeraCrypt encrypion software: https://veracrypt.codeplex.com/

[3] DataShur Personal USB Flash Drive: https://www.istorage-uk.com/product/datashur-personal/

[4] DataShur Professional USB Flash Drive: https://www.istorage-uk.com/product/datashur-pro/

[5] Eraser software: http://eraser.heidi.ie/