Government of **Western Australia**
Department of **Health**

IT Security Risks and Mitigating Controls for Research

In completing an IT Security Risk Assessment, researchers should identify the IT security risks relevant to their research proposal and what controls are in place to mitigate those risks. While the following are a guide to identify the potential risks and controls, they are not exhaustive and researchers may need to consider additional risks or controls depending on their individual proposals. Not all risks or controls will be relevant to all research proposals and some controls may assist in mitigating multiple risks.

Data refers to research data provided by the DoH, an alternative source, or as collected by the researchers themselves.

Potential Risks	**Mitigating Control Examples**
A. Researcher's organisation does not follow good IT security governance, resulting in poor IT security practices	1. The organisation's IT Security practices are regularly subject to internal, external or quality audits 2. The IT security environment is baselined against an appropriate standard eg. ISO 27001 3. An approved and up-to-date IT Security Policy is in place at the organisation 4. All users are required to adhere to an IT Acceptable Use Policy 5. All research personnel must sign a confidentiality agreement 6. Researchers are required to undertake regular IT security training 7. Researchers are required to undertake regular privacy training
B. Data is lost, corrupted or exposed while transferred to, by, or from the researcher	8. The secure electronic transfer of data should be via MyFT, SUFEX or similar 9. The faxing of paper-based records and/or data is not allowed
C. De-identified data is re-identified without appropriate approval	10. Research data is de-identified when linked and associated with a randomly assigned ID number 11. Data is de-identified and linked prior to be being used by researchers 12. Researchers do not have access to identifiable data
D. Data collected from research participants via an insecure mobile app is exposed or lost	13. Data on the app is encrypted at rest and only accessible to the user 14. App data is up-loaded to a secure server using end-to-end encryption 15. Data stored on the server is encrypted at rest and only available to the Researchers via end-to-end encryption

Potential Risks	Mitigating Control Examples
E. Data sovereignty issues result in research data stored outside of Australia being exposed or lost	16. Data resides within Australia 17. Data is encrypted at rest 18. Hosting service does not have access to encryption keys
F. Data stored on a portable device is lost or stolen resulting in exposure or loss of data	19. Data will not be transferred physically via an external drive or laptop 20. Portable drives and devices are physically secured when not in use 21. Data stored on portable drives and devices is encrypted
G. Data not used for intended purpose	22. Researchers agree data is only to be used for the study authorised by HREC and by individuals identified in proposal 23. Researchers seek approval from HREC for any changes from the agreed intended use of the data
H. Unauthorised access to hard copy files results in exposure or loss of data	24. Hard copies of data and related physical records are locked in secure physical record storage when not in use
I. Unauthorised access to researcher's personal computer results in exposure or loss of data	25. Personal computers are kept within a secure area with access restricted to researchers 26. All users are required to have a unique login and password 27. Sharing of logins and passwords between users is prohibited 28. Personal computer screens lock automatically after 5 minutes of inactivity
J. Unintended erasure or corruption of data	29. Data is regularly backed up
K. Unauthorised access to backups results in exposure or loss of data	30. Backup of data is encrypted with access restricted to authorised IT personnel only
L. Personal computers or servers subject to ransomware, malware or virus attack resulting in exposure or loss of data	31. Up-to-date anti-virus and anti-malware software is installed 32. Personal computers and servers used are configured and maintained by the organisation and automatically or regularly updated 33. Local administration access rights are limited on each personal computer to prevent unauthorised installation of software
M. Insecure remote access leads to unauthorised exposure or loss of data	34. Remote network access requires two factor authentication 35. Remote access utilises VPN or similar for secure end-to-end connection

Potential Risks	Mitigating Control Examples
N. Insecure network results in unauthorised exposure or loss of data	36. Network activity and traffic is logged and actively monitored by IT personnel 37. The network is regularly scanned for internal and external vulnerabilities 38. The network is regularly subject to external penetration testing 39. External access to the network is restricted or blocked 40. The network is protected by a firewall that is actively managed 41. Network login passwords have adequate complexity requirements e.g. minimum number and enforced mix of characters 42. Passwords are regularly required to be changed and cannot be re-used
O. Unauthorised access to data stored on a server results in exposure or loss of data	43. Entry to the physical location of the server is restricted to authorised IT personnel only 44. Access to data on the server is limited to authorised researchers only 45. Data stored on the server is encrypted at rest
P. Identifiable data is reported publicly without consent	46. Researchers ensure data pertaining to a single or particular individual will not be reported 47. Researchers ensure identifiable data will not be reported
Q. Exposure or loss of archived data prior to disposal	48. The data and records created as part of the research, are Included in a defined retention schedule as part of a managed record keeping system 49. The retained data is encrypted and stored in a managed and secure environment 50. Access to the retained data is restricted
R. Inadequate data disposal process results in failure to dispose of data or exposure of data	51. There is a documented secure digital erase procedure 52. Disposal process includes secure disposal of backups 53. There is a secure disposal process for physical records 54. Researchers to inform HREC when the data is destroyed