Patron Data Security Dos and Don'ts Guide for data applicants & recipients

Department of General Practice (DGP), Melbourne Medical School

2 April 2020

This document outlines data security requirements for the housing of Patron data by Data Recipients and contextual information for data applicants.

How to access data

If you are reading this, then chances are you are either seeking or have been granted approval to receive Patron data. If not, information on how to apply to access Patron data is on the 'Researchers' page of the Data for Decisions website, under the Communities and Data Use tab: www.gp.unimelb.edu.au/datafordecisions.

A completed Data Access Application and Data Risk Management Plan (**DRMP**) must be submitted 3 weeks prior to the meeting of a Patron Data Governance Committee.

Purpose of this information

The information in this document can assist Patron data applicants to:

- complete their Data Risk & Management Plan
- remind you of your data environment obligations once you have received Patron data.

Five Safes risk dimensions

The Patron Data Governance Committee assesses all applications with consideration of the Fives Safes which relates to safe people, safe projects, safe data, safe settings and safe outputs. The Committee may ask Applicants for additional information if they consider it necessary to fulfil their due diligence.

Data Recipients' obligations

MOU and/or Legal Agreement

DO be aware that prior to receipt of data, Data Recipients external to the University of Melbourne sign a legal agreement with the University of Melbourne (*Data Access Agreement*). The Agreement stipulates Data Recipients' compliance with the ethical, legal and regulatory obligations related to data privacy, data management and security. Researchers internal to the University sign a Memorandum of Understanding (MOU) like the legal agreement. There is a summary document explaining this on the Data for Decisions website resources page.

Data Breach

If you have access to Patron data and you become aware of a data breach, unauthorised access, loss or compromise of data:

DO notify the Patron group within three days (as per legal agreement).

DO undertake any required actions you are asked to perform.

Allowable uses for Patron data

DO apply for and use Patron data only for allowed purposes: research (incl. audit and quality improvement), education, teaching and policy.

Completion of the application & DRMP

DO be concise, accurate and specific with the information you provide in your application and DRMP. Requests for more information can delay approval.

DO provide only true and accurate information.

DO become knowledgeable about your institution's established information security policies and processes.

DO liaise with your institution's IT managers to ensure that Patron data is housed and managed with appropriately high levels of data security.

DO ask your IT provider for details about the data housing environment and safeguards that will be in place to manage Patron data, including information about:

- Access logs and automated monitoring of access
- Backup of data in appropriate ways
- Destruction of data at end of data retention
- Encryption and firewalls
- Preventing unauthorised access to or copying of data
- Mechanisms to restrict data access to authorised personnel (including two-factor authentication, read only or edit access).

DO become knowledgeable about your institution's established information security policies and processes and whether they meet the minimum requirements for Patron data housing and use.

Postal address:
Data for Decisions, Department of General Practice
University of Melbourne, VIC 3010, Australia

Phone: 03 8344 3392
Email: vicren-enquiries@unimelb.edu.au

Incorporate privacy by design

DO design data security measures with the aim to:[3]

- prevent misuse, interference, loss or unauthorised accessing, modification or disclosure of Patron data
- detect privacy breaches promptly
- be ready to respond to potential privacy breaches in a timely and appropriate manner.

Minimum data security requirements when accessing raw Patron data

DO:

☐ ensure that the data security requirements comply with those listed in your Patron Data Risk & Management Plan (DRMP). **All mandatory requirements listed in the DRMP must be met.** Complying with additional recommendations is advised (Appendix A of your DRMP).

☐ appoint an appropriately qualified and experienced Data Custodian.

☐ have a sensitive data security expert mentor your Data Custodian if your Custodian lacks sufficient experience handling sensitive data.

DON'T ever:

☐ share your login credentials that enable access to patron data with anyone

☐ store Patron data on personal hard drives, USBs or other personal or portable devices

☐ provide Patron data to any person or colleague not approved in your ethics and data access applications – unless it is in highly aggregated form ready for publication

☐ attempt to reidentify any Invidual persons whose data are in the Patron repository

Minimum data security requirements for identifiable Patron-related data

If you are running a clinical trial or other intervention study, or you intend to give feedback to consenting practices, you may have practice or person identifying information to manage.

DO:

☐ use deidentified codes to identify practices or patients and do not house the coding key with documents containing coded data

☐ house the data with similarly high security and access measures as is used for Patron data.

Data recipient training & getting help

DO

☐ Ensure that your Data Custodian receives data security and incident prevention training from a Patron group representative.

☐ Ensure that all Patron Data Recipients receive data security awareness and incident prevention training

☐ Ensure that all Patron Data Recipients have undergone appropriate ethics training

☐ Contact the Patron Management Group if you are ever unsure about anything. This includes aspects of your data storage environment, how you handle data within your team, or questions about something you have found in your data – e.g. suspected privacy breach.

☐ Contact VicREN Manager: vicren-enquiries@unimelb.edu.au Phone: 03 8344 3392

DON'T:

☐ Don't think we are too busy to take your call if you are unsure. It's better to be safe than sorry.

Definitions and Acronyms

Data Custodian A person within your project team responsible for the secure and appropriate housing and sharing of Patron data.

Data Recipient Members of the project team allowed access to Patron data and their employer organisations.

DGP Department of General Practice

DRMP Data Risk Management Plan

MOU Memorandum of Understanding

UoM University of Melbourne

Amendment, Modification or Variation

This document may be amended, varied or modified by the Department of General Practice, University of Melbourne.

References

1. Patron Data Governance Framework 2019: https://medicine.unimelb.edu.au/school-structure/general-practice/engagement/data-for-decisions#resources Accessed 19 November 2019
2. Desai, Ritchie and Welpton (2016) Five Safes: Designing data access for research UWE Bristol Research Repository. https://uwe-repository.worktribe.com/output/914745 Accessed 19 November 2019
3. Australian Government Office of the Australian Information Commissioner (2018) Guide to securing personal information. https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/ Accessed 20 November 2019