Ethics Application Guidance

Context

All Research projects seeking to access data in the Health Research Data Platform-Saskatchewan are required to submit an ethics application. To support this, the HRDP-SK has created this guide to support teams in completing their ethics application specific to the questions regarding data storage.

Questions/ Responses

Explain why the waiver of consent is unlikely to adversely affect the welfare of individuals to whom the information relates:
The data are de-identified reducing the likelihood of re-identification of individuals and accessed in a secure virtual environment which data cannot be removed without approval from data trustees and passing a vetting process that ensures anonymity. Thus, individuals cannot be adversely affected by the use of their data.

Explain why obtaining consent from individuals to whom the information relates is impractical, impossible and/or would adversely affect the research:
It is not reasonably practical to seek consent from Saskatchewan's 1.1 million residents to access their health data, and it is impossible to get consent from people who have died or left the province to access their historical records. Since this research is strictly a secondary analysis of de-identified data and is of significant benefit to the SK population, consent is not required.

Identify the research personnel responsible for abstracting data and where the data abstraction will occur:
Saskatchewan's databases are stored in a central repository on eHealth Saskatchewan's secure servers. All data is stored in Canada. eHealth will serve as the Information Service Provider as per their IMSP agreement with each data trustee. Once ethical approval is received from the REB, the project has been approved by the trustees of the data, and a research agreement has been signed by the researchers, eHealth analysts will access the central repository and extract the data within the secured eHealth network and place it in a virtual secure research environment in which the data can be safely and securely remotely accessed and analyzed for research (details on how the secure research environment operates are below).

Describe how the data will be stored (i.e., computerized files, hard copy, personal digital device, other):
Extracted data is maintained electronically within eHealth Saskatchewan's central repository. The secure research environment can only be accessed by the Information Management Service Provider and approved HRDP-SK users. Access will be via a remote, secure virtual network connection using multi-factor authentication. HRDP-SK Users will complete their data analysis within the secure research environment. A vetting process will be followed prior to the transfer of outputs being sent to the researcher outside of the secure research environment.

Describe the safeguards in place to protect the confidentiality and security of the data. If a coding procedure is being used, describe in detail:
All data are de-identified prior to being made available to HRDP-SK users. The HRDP-SK Onboarding and Account Request stage requires each user to complete privacy training, submit a conflict-of-interest declaration, a criminal record check, and sign a user agreement that includes

Ethics Application Guidance

a confidentiality agreement. All data analysis occurs within the HRDP-SK secure research environment. Remote access to the secure research environment is password protected, times out when idle, and restricts the ability to remove data from that environment (e.g. no internet access, disabled USB ports, etc.). Prior to allowing analytical results to leave the secure research environment, the results are independently vetted by an eHealth team member to ensure it meets privacy requirements (e.g., release aggregate date only, suppress cells/statistics representing less than 6 patients). The vetting process will ensure that all identifiable or re-identifiable data remains in the secure research environment.

Identify the research personnel responsible for safeguarding the link to the source data (I.e. master list):
All secondary data are de-identified prior to being made available to the HRPD-SK. Thus, there is no master list.

Describe the storage arrangements, including the data retention period and final disposition of the data:
In conjunction with applicable laws, a Master Health Data Sharing Agreement between the partner organizations of the Ministry of Health, the Saskatchewan Health Authority, Saskatchewan Cancer Agency, Saskatchewan Health Quality Council, eHealth Saskatchewan, Saskatchewan Association of Health Organizations, and 3sHealth has been established that stipulates expectations for protection individuals' privacy in the use and storage of the data, as well as any reporting based on the data. Data storage and retention is described above. Datasets created for this project will be stored on the HRDP-SK secure server in a folder that contains the purge date in its name (e.g., StudyName_PURGE31DEC2021), which will be 2 years after the project closure date. The folder will be deleted using the purge date and a file eraser/overwriting program will be run to permanently delete the data within one month of the purge date.

Confirm that the Lead Principal Investigator will be responsible for the storage of data. If not, specify why not, and indicate who will be responsible for data storage:
eHealth as the Information Management Service Provider for the trustees of the data made available by the HRDP-SK is responsible for the storage and safeguarding of the data.

Ethics Application Guidance

Figure 1. *Additional bulleted security safeguards identified in the University of Saskatchewan REB Biomedical Application Secondary Use of Health Data Form.*

Mitigation Safeguards to Privacy Risks

Identify the safeguards/solutions to mitigate the risk to privacy.

Safeguards/Solutions (check all that apply)

- ☒ Project personnel screening/agreements
- ☒ Access authorization procedures
- ☒ Designated systems administrator
- ☒ Passwords/screen timeouts
- ☒ System access audits/disclosure logs
- ☐ Secure mail/transport
- ☒ Firewall/virus protect
- ☒ Encrypted transmission
- ☐ Data collection tool and Master list stored in separate locations

- ☒ Aggregation levels
- ☐ Alternate identifiers

- ☒ Use of non-linkable elements or identifiers

- ☐ Confidentiality and security agreements for out-of-province recipients or storage providers

If applicable, describe any other mitigating strategies:

Additional recommendations

- It is commonplace to provide an appendix indicating the specific variable fields which will be accessed for the analysis. This must be in alignment with the information provided HRDP-SK Stage 2 Form.