APPENDIX A: DATA MANAGEMENT

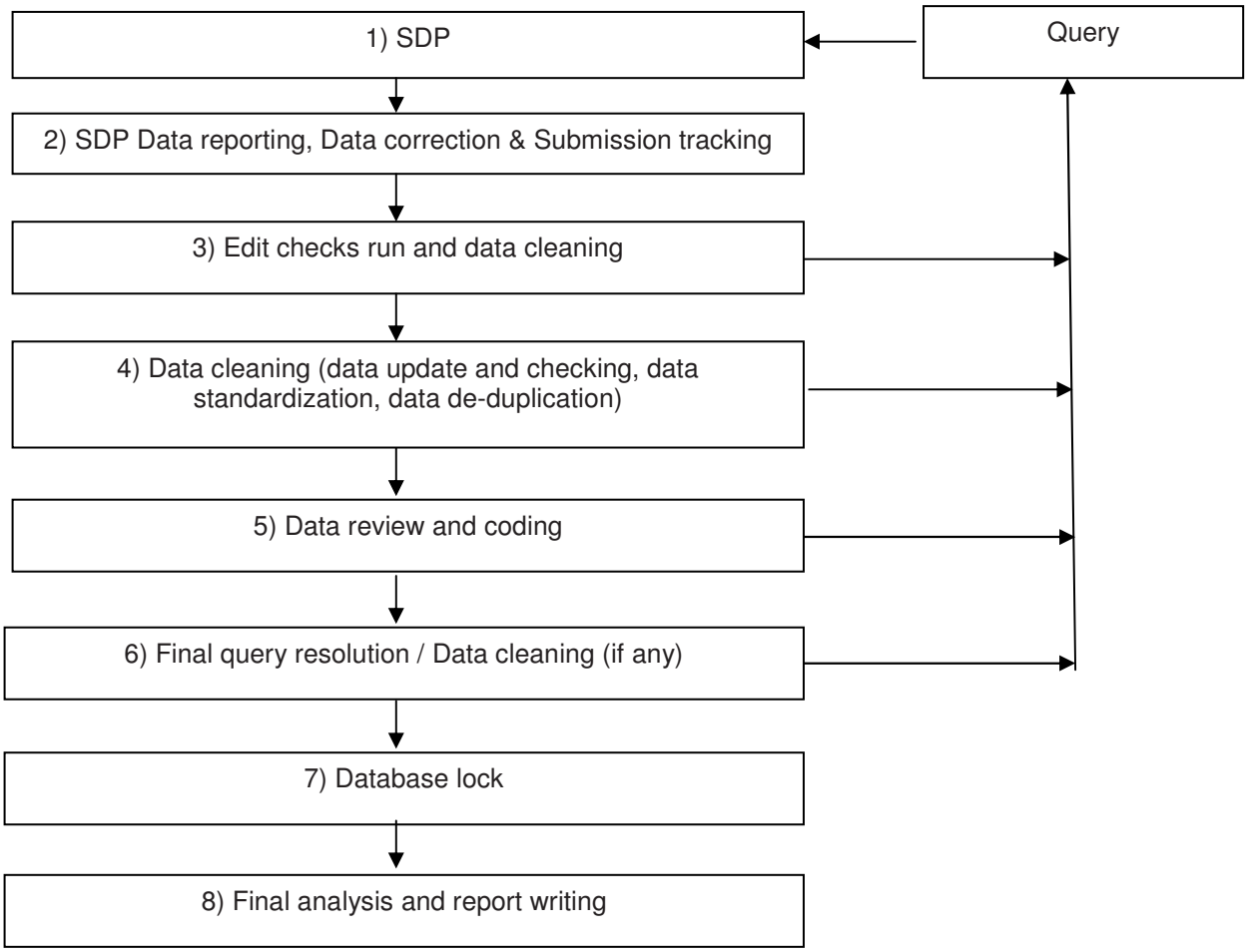
The National Cardiovascular Disease Database (NCVD) Registry maintains two different databases for cardiovascular disease, i.e. for Acute Coronary Syndrome and Percutaneous Coronary Intervention. Data is stored in SQL Server due to the high volume of data accumulated throughout the years.

Data sources

SDPs or Source Data Providers of NCVD-ACS registry comprise of hospitals with cardiologists and physicians who participated in the registry throughout Malaysia.

Data Flow Process

This section describes the data management flow process of the National Cardiovascular Disease Database Registry.



SDP Data reporting, Data correction and Submission tracking

Data reporting by SDP is done via Web Applications e-Case Report Forms.

There are a number of data security features that are designed into NCVD web application (eCRF) such as web owner authentication, 2-level user authentication (user name and password authentication and a Short Messaging System (SMS) of authorization code to mobile phone authentication), access control, data encryption, session management to automatically log off the application, audit trail and data backup and disaster recovery plan.

SDP submits NCVD-ACS Notification form on ad hoc basis whenever there is a case. SDP also submits follow-up data at 30 days, 1 year and other ad hoc follow-ups post notification date. An alert page containing all the overdue submissions for follow up at 30-day and 1-year post notification date is available to users to ease submissions tracking.

Prior to registering a patient record, a verification process is done by using the search function to identify if the patient exists in the entire registry. The application will still detect a duplicate record if the same IC number is keyed in should the step of searching patient be left out. This step is done to avoid duplicate of records. For patients that exist in the database, SDP merely needs to add a new ACS or PCI notification with basic patient particulars pre-filled based on existing patient information in the database. ACS and PCI share the same patient list.

There are a few in-built functionalities at the data entry page that serve to improve data quality. One such function is the auto calculation which is to reduce error of human calculation. There is also a function for inconsistency check that disables certain fields if these fields are answered in a certain manner. When value entered is out of range, user is prompted for the correct value.

A real-time data query page is also available via the web application to enable user to check which of the non-compulsory data is missing, out of range and inconsistent. A link is provided on the data query page for the user to click on to resolve the query for the particular patient.

Real-time reports are also provided in the web application. The aggregated data reports are presented as tables and graphs. The aggregated data reports are typically presented in two manners, the first as centre's own data aggregated data report and second as registry's overall aggregated data report. This way, the centre is able to be compared against the overall registry's average.

Data download function is also available in the web application to allow users to download their own centre's data for all the forms entered for their own further analysis. The data are downloadable as Text - tab delimited (.txt) format, Microsoft excel workbook (.xls) and Comma separated value (.csv) format.

Edit checks run and Data cleaning

Edit check was performed periodically by the registry manager to identify missing compulsory data, out of range values, inconsistency data, invalid values and error with de-duplication. Data cleaning is then performed based on the results of edit checks. Data update and data checking of the dataset are performed when there is a query of certain fields whenever necessary. It could be due to request by user, correction of data based on checking from data query in eCRF or after receiving results for preliminary data analysis. During data standardization, missing data are handled based on derivation from existing data. Data de-duplication is also performed to identify duplicate records in the database that might have been missed by SDP.

Final query resolution / Data cleaning / Database lock

A final edit check run was performed to ensure that data is clean. All queries were resolved before database is locked to ensure data quality and integrity. Final dataset is subsequently locked and exported to the statistician for analysis.

Data analysis

Please refer to section on Statistical Methods section for further details.

Data release policy

One of the primary objectives of the Registry is to make data available to the cardiovascular healthcare providers, policy makers and researchers. The Registry would appreciate that users acknowledge the Registry for the use of the data. Any request for data that requires a computer run must be made in writing (by e-mail, fax, or registered mail) accompanied with a Data Release Application Form and signed Data Release Agreement Form. These requests need prior approval by the Advisory Board before data can be released.

Registry ICT Infrastructure and Data centre

The operations of the NCVD are supported by an extensive ICT infrastructure to ensure operational efficiency and effectiveness.

NCVD subscribes to co-location service with a high availability and highly secured Internet Data Centre at Cyberjaya in order to provide NCVD with quality assured Internet Hosting services and state-of-the-art physical and logical security features without having to invest in costly internal data centre setup. Physical security features implemented includes state of the art security features such as anti-static raised flooring, fire protection with smoke and heat alarm warning system, biometric security access, video camera surveillance system, uninterrupted power supply, environmental control, etc.

Other managed security services include patch management of the servers, antivirus signature monitoring and update, firewall traffic monitoring and intrusion detection, security incidence response, daily, weekly and monthly basis data backup service, at least once yearly data recovery simulation to verify that backup works, half-yearly network security scan and penetration test, security policy maintenance, maintenance and monitoring of audit trail of user access, etc. Managed system services are also provided and these include usage and performance report, operating system maintenance and monitoring, bandwidth monitoring and systems health monitoring.