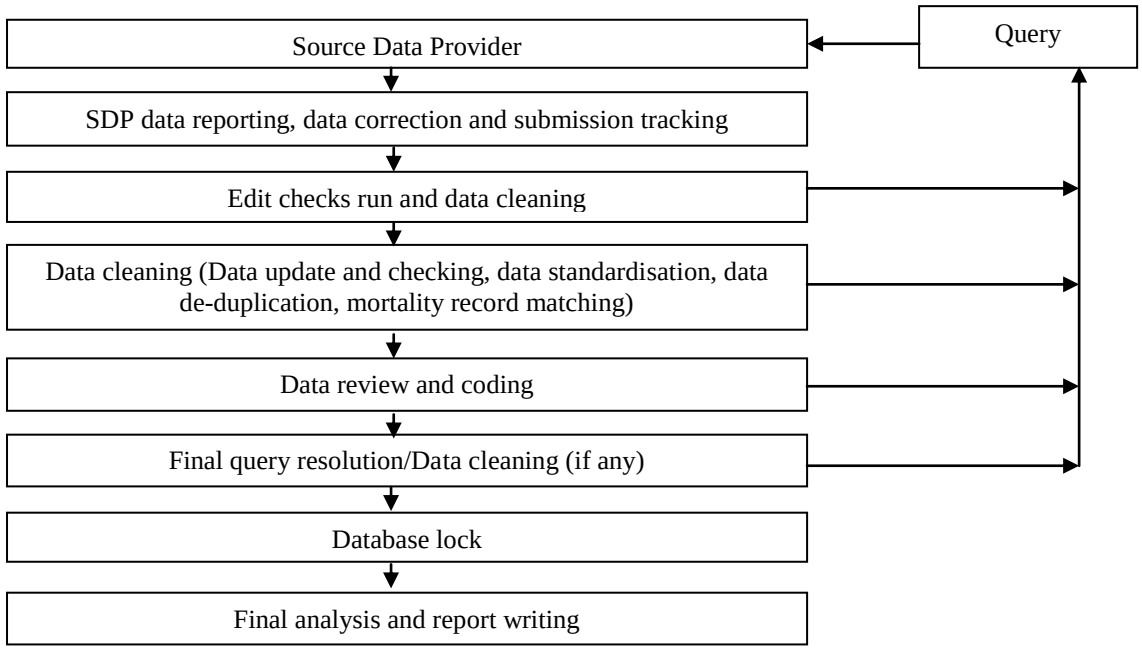
APPENDIX A: DATA MANAGEMENT

The National Cardiovascular Disease Database (NCVD) Registry maintains two different databases for cardiovascular diseases, 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
Source Data Providers (SDPs) of NCVD-PCI registry comprise all major hospitals who participated in the registry, throughout Malaysia.

Data Flow Process
This section describes the data management flow process of the National Cardiovascular Disease Database.



SDP data reporting, data correction and submission tracking
Data reporting by SDP is done via web applications e-Case report forms.

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

For PCI, SDP submits NCVD-PCI notification form on an ad-hoc basis whenever a procedure is performed. SDP also submits follow-up data at 30-day, 6-month and 12-month post notification date intervals. An alert page containing all the overdue submissions for follow-up at 30-day, 6-month and 12-month post notification date is available to users to facilitate submissions tracking.

Prior to registering a patient record, a verification process is done by using the search functionality to search if the patient already exists in the entire registry. The application will still detect a duplicate record if the same MyKad number is keyed in, should this step be missed. This step is done to avoid duplicate records. For patients' whose records already exist in the database, SDP needs only to add a

new PCI notification with basic patient particulars pre-filled, based on existing patient information in the database. The PCI and ACS registries share the same patient list.

There were a few in-built functionalities at the data entry page that serve to improve data quality. One such function is auto calculation to reduce human error, in calculations. There is also an inconsistency check functionality that disables certain fields and prompts the user, if the value entered is out of range.

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

Real time reports were also provided in the web application. The aggregated data reports are presented in tables and graphs. The aggregated data reports are typically presented in two manners, one as centre's own data aggregated data report and another as the registry's overall aggregated data report. In this way, the centre is able to compare itself 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 from all the forms entered, for their own further analyses. The data are downloadable in Text-tab delimited (.txt) format, Microsoft excel workbook (.xls) and as Comma separated value (.csv) format.

Edit checks run and data cleaning
Edit checks is performed periodically by the registry manager to identify missing compulsory data, out-of-range values, inconsistency of data, invalid values, and errors with de-duplication. Data cleaning is then performed based on the results of edit checks. Data update and data checking of the dataset were performed when there is a query of certain fields as and when necessary. It could be due to request by user, correction of data based on checking via data query in eCRF or after receiving results for preliminary data analysis. During data standardisation, missing data were 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 out by SDPs. Finally, matching the record against the National Death Register *(Jabatan Pendaftaran Negara)* database is performed to verify the mortality status of the patient.

Final query resolution/data cleaning/database lock
A final edit check run is performed to ensure that the data is clean. All queries will be resolved before the database is locked, to ensure data quality and integrity. The final dataset is subsequently locked and exported to the statistician for analysis.

Data analysis
Please refer to the Statistical Analysis Method 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 operation of the NCVD is 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 data centre setup internally. 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, data backup service done on a daily, weekly and monthly basis, data recovery simulation to verify that the backup works, which is done at least once yearly, network security scan and penetration test done on a half-yearly basis, security policy maintenance, maintenance and monitoring of audit trail of user access, etc. Managed system services such as usage and performance report, operating system maintenance and monitoring, bandwidth monitoring and systems health monitoring were also provided.