Data integrity guidelines for health services

June 2018
Contents

Introduction ........................................................................................................................................... 4
Health data ............................................................................................................................................ 5
Data integrity requirements of health services.................................................................................... 6
Governance ............................................................................................................................................ 6
Oversight ................................................................................................................................................ 6
Information technology ......................................................................................................................... 7
Health service internal auditing ........................................................................................................... 7
Selecting records for internal audit ..................................................................................................... 7
Data integrity initiatives of the Department and VAHI ................................................................. 8
Health Data Integrity audit program .................................................................................................... 8
Implementation of health data integrity audit recommendations by health services ....................... 8
Department and VAHI internal data integrity practices ...................................................................... 8
Clinical coding standards and ratified advice ....................................................................................... 9
Health data integrity audits – evidentiary standards and tolerances ............................................. 10
References ............................................................................................................................................ 11
Further reading ..................................................................................................................................... 11
Introduction

The guidelines provided in this document have been prepared in conjunction with the Department of Health and Human Services (the Department) to assist health services in meeting the requirements for integrity in the data provided by health services concerning their activity and performance.

The World Health Organization (WHO) has defined data integrity in the following terms:

‘Data integrity is the degree to which data are complete, consistent, accurate, trustworthy and reliable and that these characteristics of the data are maintained throughout the data life cycle. The data should be collected and maintained in a secure manner, such that they are attributable, legible, contemporaneously recorded, original or a true copy and accurate. Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles and good documentation practices.’

The guidelines have been compiled from formal directions to health services concerning practices, procedures and processes designed to provide assurance about the reliability of data reported to the Department. Instances of health service good practice identified through the Health Data Integrity (HDI) work program, and other means such as literature searches, have also been incorporated.

The HDI program is subject to continuing refinement based on expanded data analytics and risk assessment processes, and is guided by potential expansion of Activity Based Funding.

Health services are encouraged to ensure their governance and oversight of data and information management practices are fully compliant with these data integrity guidelines.

The guidance provided in this document is periodically reviewed and updated, particularly as information technology applicable to the health sector evolves.

Health services should view the content of this document as indicative of the base level data integrity requirements necessary to provide assurance that data reported to the Department for both performance and funding purposes are accurate and fit for purpose.

Readers are also encouraged to refer to the Victorian Public Service (VPS) Data integrity manual, published by the Department of Treasury and Finance.

Enquiries and suggestions can be addressed to Health Data Integrity, Victorian Agency for Health Information.
Health data

Activity and performance data reported by health services are used for a range of important purposes. They range from satisfying Victoria’s reporting obligations under the National Health Reform Agreement, supporting improvement in quality and safety, monitoring health service performance and viability, and service planning.

The data are also used for reporting to the Government and the Victorian community concerning the performance of the Victorian health system. They are a key element of accountability to both Government and the Victorian community.

Other significant uses include research, particularly epidemiology, and studies intended, among other things, to improve health outcomes for the Victorian community.

Health services themselves use both internally produced data and data from the Department and the Victorian Agency for Health Information (VAHI) for their own performance monitoring purposes, together with benchmarking and planning purposes.

It is therefore crucial that data reported centrally by health services reflect a strong commitment to data integrity practices supportive of high quality data.

The Department provides comprehensive documentation for the information and guidance of health services and agencies providing data to the key health datasets:
- Victorian Admitted Episodes Dataset (VAED)
- Victorian Emergency Minimum Dataset (VEMD)
- Elective Surgery Information System (ESIS)
- Victorian Cost Data Collection (VCDC)
- Victorian Integrated Non-Admitted Health dataset (VINAH).

These are available at http://www.health.vic.gov.au/hdss/. Manuals and related documentation for other datasets are also available on this website.
Data integrity requirements of health services

In order to ensure greater reliability and confidence in data concerning the Victorian health system, health services have been advised of some specific data integrity actions taken by the Department. They have also been advised of requirements expected to be implemented by health services in the context of data reported externally by the health service.

The requirements listed below represent the minimum generic requirements required of health services to ensure the integrity of data reported concerning the health system. These requirements are consistent with the delivery of high quality data from an environment where data integrity is a key aspect of day-to-day operations.

**Governance**

Health service boards are accountable for the accuracy of the data their health service reports, ensuring that data are subject to appropriate controls over data accuracy. Boards are expected to make this a responsibility of their audit committees.

**Oversight**

Health services are to:

- provide advice to patients on the elective surgery waiting lists of any change to their status or their surgery date
- record in the system the name of the health service senior clinician authorising a change to previously recorded data at the time of the change being made
- undertake regular process reviews of data recording and reporting practices, particularly relating to required authorisation for changes to data
  
  - ensure separation of functional responsibility and management oversight for data collection management, data extraction, and submission to the Department
  - maintain a record of approval from a health service’s nominated senior manager or executive for each dataset submission to the Department
  - conduct annual reviews of their internal policies and procedures related to data management, triggered by the Department’s annual release of updated data collection manuals.

Health service board of management audit committees are responsible for oversight of internal audits of source data and related systems and processes for all externally reported data to the Department.

In addition, health service boards are also required to provide a statement in their annual report to Parliament that they have appropriate systems and processes in place to assure the quality of reported data.
Information technology

• All health service staff using health service data recording and reporting systems must be uniquely identified.

• Recording of all entries and changes to health service data in transaction logs/audit trails such that the user creating or amending the data can be identified, the original value and changed value are recorded and the date and time of the change are recorded.

• Regular review by health services of access control registers for systems that hold health data to ensure that access is only provided for staff with a genuine business requirement. These reviews are required to identify and validate user access and facilitate effective logging of changes to data.

• Regular checking of system controls and their use, in particular ensuring that user identifiers and passwords are not being shared.

• Comprehensive testing of new systems or existing system updates prior to implementation to ensure data integrity is maintained.

• Regular backups are undertaken and maintained in such a manner that would allow successful recovery when required.

DHHS Sector Assurance, Digital Health branch has also established a set of baseline cybersecurity controls for health services. These cannot be specifically detailed here as many of these cybersecurity controls cover secure access to, and management of, health data. Access to the controls is via Health Service Chief Information Officers or the Manager, Health Sector Assurance Digital Health branch of the Department. Health services must comply with all of the controls.

Health service internal auditing

Part of health services’ responsibility for data accuracy and quality/integrity in the context of regular submissions of data to the Department involves periodic auditing and evaluation of their data management practices, including internal processes, oversight, governance and data quality assurance.

Design of audits, evaluations and quality inspections is largely predicated on factors such as:

• a known or suspected quality issue
• the need for assurance about the quality and reliability of reported data
• establishing confidence that internal processes, governance and oversight are robust
• whether an indicative measure of accuracy is required.

Selecting records for internal audit

In undertaking their own data integrity audits, once the scope of the audits are determined, health services will need to consider the approach to selection of patient records for auditing.

The Department and VAHI’s external audits have used a random and targeted mix of sampling strategies depending on the type of auditing being undertaken and the type of result sought.

Under the new Health Data Integrity (HDI) Program plan 2018–19 to 2019–20, VAHI will conduct desktop analysis for routine surveillance of datasets and key variables within datasets and to identify statewide or health service-specific issues requiring investigation. VAHI will make the results available to senior representatives of the relevant health service(s) in the first instance, to ensure a shared understanding of the matters under review. The selection logic used to derive this information will also be made available to health services for (adaptation to) internal use as required.
Data integrity initiatives of the Department and VAHI

Health Data Integrity audit program

Health data integrity audits of public health services have been conducted in Victoria since 1993. The first audits principally related to clinical coding of admitted data, coinciding with the introduction of casemix funding of Victorian hospitals. These audits of admitted data have continued since.

Subsequently, health data integrity auditing of data reported centrally by health services was extended to the VEMD and the ESIS datasets and further datasets have since been added. In addition, targeted, or spot, audits at health services have been conducted.

The audits provide assurance concerning, firstly, the validity of data used in casemix funding of Victorian health services. They also show the reliability of data reported concerning the performance of Victorian health services and the health system generally.

The audits also review, and report upon, health services’ compliance with these guidelines.

Audits of the key health datasets will continue in coming years. VAHI has introduced a risk-based approach to development of the audit programs, together with an enhanced approach to data analytics to support more effective targeting of the audit effort.

Health services are expected to actively participate in the program of independent, system-wide inspections, checks and audits of their health service data and related processes conducted by VAHI, including responding to data analytics queries.

Implementation of health data integrity audit recommendations by health services

Reports of individual audits are provided to health services in draft form following the completion of audit fieldwork. Health services provide responses, including action plans, to audit recommendations. These are included in the final audit reports, provided to health services’ CEOs by VAHI.

VAHI periodically requires advice from health services of their progress with implementation of audit recommendation action plans, including evidence demonstrating implementation of recommendations for issues that carry a high risk impact.

Initial and final health service responses to audit recommendations, together with details of supporting evidence from health services, are maintained in VAHI’s Health Data Integrity audit recommendations database.

Department and VAHI internal data integrity practices

Through many years of experience in the management of key health datasets, the Department and VAHI have identified and implemented steps to ensure the processes and practices relating to management of data reported by health services are of the highest standard.

The processes and practices intended to ensure the integrity of data after receipt from health services include the following:

- Comprehensive manuals, reviewed annually, are provided for the guidance of health services, software vendors and users of the data, as well as Department and VAHI staff.
• Formal records are maintained of any changes to submission files (source data) requested by health services and processed by the Department for a period of three years.

• A validation regime, described in detail in the data collection manuals, is applied to submitted data from health services.

• Permanent secure storage of the original submissions of data are maintained for auditing purposes for a period of three years.

• Logging of transmission events is maintained (file received/report sent, users, dates etc.) for a period of three years.

• Data integrity practices conform with page 7 of the VPS Data integrity manual (to which all data validation procedures must comply).2

• Change control processes have been specified to ensure that authorisation of changes to validation procedures is maintained.

• Regular checking of original submissions against final warehoused data is undertaken to ensure the integrity of the validation and transformation/derivation steps. In addition, regular analysis of data is undertaken after validation processing, to identify outliers, inconsistencies, variance between time periods and apparent unusual patterns in output data.

• Surveillance of datasets and key variables within datasets performed by VAHI, to identify statewide or health service-specific issues requiring further investigation.

• Liaison by both the Department and VAHI with health services about data integrity, including developing and promoting data integrity best practice (these guidelines are an example).

• Implementation of data integrity audit recommendations provided by auditors for the attention of the Department or VAHI is monitored by the Department’s Audit and Risk Management Committee.

• The Department and VAHI Data Quality includes a Data Quality Policy, a Data Quality Improvement Standard Operating Procedure and a range of templates for capturing, tracking, measuring and summarising data quality issues.

Clinical coding standards and ratified advice

The Australian Consortium for Classification Development (ACCD) publishes the Australian Coding Standards (ACS)3 with each update to the International Statistical Classification of Diseases and Related Health Problems, Tenth Revision, Australian Modification (ICD-10-AM)4 and Australian Classification of Health Interventions (ACHI) classifications.5 The standards provide comprehensive guidance for clinical coding and prescribe coding conventions for use with the ICD10-AM and ACHI classifications. They provide a cornerstone for quality improvement of clinical coding and include, as an appendix, Standards for ethical conduct in clinical coding.

To supplement the Australian Coding Standards, the Victorian ICD Coding Committee (VICC) publishes the Victorian additions to the ACS annually.

Additionally, the ACCD and the VICC publish quarterly coding advice in response to coding queries received from clinical coders. The advice from these quarterly publications is to be applied by health services along with the ACS and Victorian additions to the ACS. It is these standards and ratified advice that are used as references in the auditing of coding accuracy.

Health services should also refer to the Standards for ethical conduct in clinical coding in the appendix in the ACS and the accompanying Clarification on the application of the “Standards for ethical conduct in clinical coding” document published in October 2017 with respect to the ethical practices that are core to the clinical coding role to ensure the integrity of coded clinical data.6
Health data integrity audits –
evidentiary standards and tolerances

Based on experience gained in data integrity audits at health services in recent years, the Department has developed a suite of evidentiary standards and tolerances to apply when conducting audits of health data. The standards are shown in Table 1.

Table 1: Endorsed evidence standards and time tolerances for application by auditors

<table>
<thead>
<tr>
<th>Standard or tolerance</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Where times recorded in VEMD and in (hard copy) source patient records differ, a tolerance of five minutes (plus or minus) is allowable.</td>
<td>This tolerance acknowledges the dynamic nature of the emergency department work environment that can lead to delays in data recording.</td>
</tr>
<tr>
<td>2. Where departure times from an emergency department for patients transferred to ward cannot be determined from the emergency department patient record, a tolerance of up to one hour is permissible between the VEMD reported time and the time notes/observations are first made in the patients inpatient file.</td>
<td>While emergency department departure time is always expected to be recorded, in practice it may be overlooked. The tolerance makes a realistic allowance for missing emergency department departure time and is based on the VAGO precedent from their Access to Public Hospitals: Measuring Performance audit, published in April 2009.</td>
</tr>
<tr>
<td>3. Where items are recorded in VEMD as ‘Null’, but information exists in the medical records to indicate that data is available, VEMD data is treated as not agreeing to medical records.</td>
<td>In particular, emergency department data recording practices are changing as IT systems evolve. This standard acknowledges that some emergency departments are moving to higher levels of reliance on IT systems.</td>
</tr>
<tr>
<td>4. Subject to the required controls for authorisation of data changes, user identification and verification and system transaction logging being met, electronic patient records are acceptable verification for health data audits purposes.</td>
<td>This standard acknowledges the ‘benefit of the doubt’ should remain with health services and is based on the VAGO precedent from their Access to Public Hospitals: Measuring Performance audit, published in April 2009.</td>
</tr>
<tr>
<td>5. Where items of data reported to Department data collections are not able to be validated in either hard copy or electronic patient records, the content of those data items are not treated as an exception.</td>
<td>The Department has advised health services that it is not necessary to maintain file copies of all correspondence, as long as definitive IT system evidence of the correspondence exists.</td>
</tr>
</tbody>
</table>

Most of these standards have particular application to specific data collections. However, they are indicative of the minimum evidentiary standards and tolerances that health services are expected to observe in data collection, recording and reporting activities.
References


Further reading

Comprehensive manuals for the key health data collections can be found at http://www.health.vic.gov.au/hdss/.

Additional reading relating to health data integrity is listed below:
