TECHNICAL SPECIFICATION

ISO/TS 20405

First edition
2018-05

Health informatics — Framework of event data and reporting definitions for the safety of health software

Informatique de santé — Cadre des données relatives aux événements et de compte-rendu des définitions pour la sécurité des logiciels de santé

Reference number
ISO/TS 20405:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Introduction

Patient safety is a major, worldwide concern in healthcare.

Individuals and organizations representing an array of roles, responsibilities, interests and relationships have become involved, including clinical professionals, academic researchers and patient advocates, as well as government and health regulatory authorities, and of course public and private sector corporations delivering healthcare.

Since 1999, patient safety has been a consistent focus of deliberation and action at national and international levels, including at ISO and IEC. Existing standards have been revised and new ones developed to incorporate recognized and emerging best practices in patient safety, in particular with respect to risk analysis, prevention and mitigation.

While these efforts have been supported by local, regional and global initiatives to improve patient safety, a consensus-based framework approach to the identification and reporting of incidents, near-misses and unsafe conditions with respect to the safety of health software has not been articulated. This is a significant gap when considering:

1) the rapidly increasing use of health information technology (HIT) in healthcare delivery,

2) the greater uptake and implementation of products on a more global basis, and

3) the rapidly expanding endeavour towards achieving greater interoperability, based on standards and specifications, of previously 'stand-alone' or otherwise heterogeneous health software systems.

Considering this gap, it is useful to return to the Institute of Medicine's report[[16]]which noted that improved surveillance mechanisms are needed to identify, capture, and investigate adverse events to continually improve the safety of HIT.

In the context of achieving a framework approach, it is important to understand that the use of the term “Identification” in this document refers to the capacity to describe health software safety events, in suitable quantitative and qualitative fashion through concepts, definitions, and processes, so as to provide the most useful information in support of current and future efforts to avoid or mitigate patient safety incidents.

Indeed several nations already have a variety of general and specific reporting regimes with respect to the safety of health software, including but not limited to the Agency for Healthcare Research and Quality's (AHRQ) common formats approach, the National Health Service (NHS) England's National Reporting and Learning System (NRLS), Japan's Medical Near-Miss/Adverse Event Reporting Project, among many others (see Annex A). Academic research in this area is also growing, including the classification for problems associated with IT systems in healthcare. These regimes as well as academic research have helped greatly in the preparation of this document.

This document is based upon a primary focus of patient safety. It is therefore principally concerned with setting out suitable definitions that describe data in most/all events where health software performs adversely (either in a stand-alone sense, or when interoperability is involved between distinct systems) and thereby poses a risk to patients.

Using this framework approach, it is anticipated that incidents, near-misses and unsafe conditions involving the safety of like or similar health software systems can better be defined, documented and compared, with the result being a greater, shared understanding of health software, systems safety risks and better informed actions to both mitigate future risks and respond when adverse actions occur. Use of incident data can have a broader relevance to the notification and response to events that results from any of the event classifications.

This document does not describe how learning from incidents should be managed. There might be a risk that separate analyses of incidents, complaints and other health software-related adverse events can result in fragmented solutions that do not address problems effectively. A combined analytical and

resolution framework approach, involving incident data along with data from other relevant sources, can therefore be considered.

Health informatics — Framework of event data and reporting definitions for the safety of health software

1 Scope

This document provides a model framework for improving the surveillance and reporting of events with respect to the safety of health software.

This document defines those data elements needed for identification of particular events including incidents, near-misses and unsafe conditions, as well as outlining good principles, relevant concepts and a process model for the recording, analysis and reporting of event-specific information related to the safety of health software.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
hazard
potential source of harm

[SOURCE: ISO/IEC Guide 51:2014, 3.2]

3.2
hazardous event
event that can cause harm

[SOURCE: ISO/IEC Guide 51:2014, 3.3]

3.3
health software
software intended to be used specifically for managing, maintaining or improving health of individual persons, or the delivery of care

[SOURCE: IEC 82304-1:2016, 3.6]

3.4
health software safety event
hazardous event involving, either directly or indirectly, the operation of health software that risks the safety of the patient

3.5
incident
patient safety event that reached the patient, whether or not the patient was harmed

[SOURCE: AHRQ Common Formats for Event Reporting – Users' Guide, May 2017]

3.6
incident management
defined process for logging, recording and resolving incidents

[SOURCE: Information Technology Infrastructure Library, 2011 Edition]

3.7
near-miss
patient safety event that did not reach the patient

[SOURCE: AHRQ Common Formats for Event Reporting – Users' Guide, May 2017]

3.8
monitoring
continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

[SOURCE: ISO Guide 73:2009, 3.8.2.1]

3.9
safety
freedom from risk which is not tolerable

Note 1 to entry: Health software's role in contributing to iatrogenic harm to patients can be direct (i.e. the design does not meet intended use requirements) or indirect (i.e. the design meets intended use requirements but the system was not configured properly). In the context of patient safety, this involves the reduction of risk of harm associated with health software to an acceptable minimum.

[SOURCE: ISO/IEC Guide 51:2014, 3.14]

3.10
unsafe condition
circumstance that increases the probability of a patient safety event occurring

[SOURCE: AHRQ Common Formats for Event Reporting – Users' Guide, May 2017]

4 Principles, data concepts and process model

4.1 General

The framework of event data and reporting definitions for the safety of health software is premised upon key principles, data concepts and a process model. Using these components, an organization can understand the rationale and methodology to undertake a structured effort in establishing or improving upon the recording, analysis and reporting on incidents, near-misses and unsafe conditions as these relate to the safety of health software.

It is important to note that this document takes an organizational focus in describing the actions necessary for the definition and implementation of the framework's components, as the adoption and implementation of the framework should be a strategic decision of an organization. That said, there are important leadership and participation roles within the framework for individual stakeholders and interests whether these are in the context of an organization, e.g. as an employee or contractor, or as an organization-independent or 'public-at-large' individual.

Finally, it is also important to note that numerous nations have laws and regulations, and regional and international organizations have mutually-binding agreements with respect to the safety of health

software in general, and its surveillance in particular. The consideration and use of this document shall respect those laws, regulations and agreements accordingly.

4.2 Principles

4.2.1 General

A principle-based approach is useful to structure the overall framework of event data with respect to the safety of health software in the context of incident management, extending to the specific use (i.e. action) of the data by the organization, as well as any involved or interested parties including but not limited to the health software vendor, jurisdictional and regulatory authorities etc., as well as for ongoing vigilance and further corrective responses (i.e. monitoring and review).

In total, these principles should contribute towards a data-driven framework that supports the overall goal of available, useful and safe health software for clinicians and other end-users involved in caring of patients.

4.2.2 Proactivity

To ensure the effective and efficient surveillance and reporting of events with respect to the safety of health software, an organization's approach shall be established in advance, optimally at the initial stage of determining the need for health software, and as a necessity before its commissioning and use.

4.2.3 Objectivity

The organization shall ensure an impartial approach to the recording, analysis and reporting of event-specific data related to the safety of health software. It shall be driven by and act at all times without bias and in the best interests of patients, towards the principle of 'primum non nocere' ('first, do no harm').

4.2.4 Accountability

The organization shall ensure that all staff involved with the operation of health software are mandated to, and supported in their responsibility in the recording, analysis and reporting of event-specific data related to the safety of health software, and in particular in the timely detection and communication of safety events by staff at large in the organization.

It is important that, in setting this mandate and supporting the accountability of staff, the organization fairly consider and as appropriate adopt a non-punitive, i.e. a 'blameless and shameless' approach. The organization should therefore initiate and sustain an atmosphere of trust, in which the candid identification and communication of health software safety events is particularly encouraged and espoused. This will result in a responsive culture that proactively instils the desire for staff to take action.

4.2.5 Transparency

The organization shall ensure that it is evident and unambiguous in all aspects of the recording, analysis and reporting of event-specific data related to the safety of health software. While respecting the privacy and confidentiality of all personal health information, the organization shall work towards staff, jurisdictional and regulatory authorities, as well as the public, being able to see what actions are being performed to ensure the safety of health software.

4.2.6 Preparedness

The organization shall establish and maintain such policy, procedures and processes so as to be ready for the recording, analysis and reporting of event-specific data related to the safety of health software. This timely planning and preparation shall include, but not be limited to, the following:

— scope and oversight over health software operated or used by the organization, and

— generally communicating and specifically orienting as appropriate all organization staff.

4.2.7 Comprehensiveness

The organization shall ensure that its overall approach to the recording, analysis and reporting of health software safety events is complete and inclusive so as to achieve a sustained and ongoing enterprise approach involving the perspectives of like or similar health software as it is used by the organization over the full software life cycle, from the initial planning to final decommissioning.

The organization shall also ensure that, over time, a complete log of data involving the recording, analysis and reporting of health software safety events is maintained. This log should also include all data related to any action, monitoring and review taken by the organization as well as lessons learned involving the safety of health software.

NOTE An ongoing comprehensive approach can facilitate an organization's systematic management of health software safety and, in particular, can enable an institutional memory that is independent of elements and factors that can change over time, such as the arrival or departure of staff, the implementation of new policies and processes.

4.3 Data concepts

4.3.1 General

As with any data-driven reporting framework, there are key concepts that support the data being optimal or fit for the intended purpose in the recording, analysing and reporting of health software safety events. Data that is fit for the intended purpose requires ongoing vigilance as existing health software evolves, new health software is introduced into use, and old health software is decommissioned.

Where appropriate, data shall be comparable and compared for consistency, e.g. through such means including but not limited to inter-rater reliability checks where recording involves the assessment and judgement of an individual or group. Any discrepancies shall be addressed accordingly.

4.3.2 Accuracy

The organization shall ensure that all data reflects the purpose for which it was designed to measure.

4.3.3 Timeliness

The organization shall ensure that all data are current and relevant.

NOTE Data timeliness can be assessed by measuring the gap between the end of the reference period to which the data pertains, and the date on which the data becomes available to users who are thus informed and can take action as necessary.

4.3.4 Comparability

The organization shall ensure that all data are comparable.

NOTE Comparability involves the extent to which data are consistent over time, and also the use of standard conventions, such as data elements or reporting periods, making them comparable to other data collected over other time periods and for different circumstances, e.g. for the same or similar health software operating in the same or a different care venue(s).

4.3.5 Usability

The organization shall ensure that all data are usable, and is easily accessible and understood.

NOTE In the context of the safety of health software, usability can be affected by the amount of data collected with respect to a specific event; it can also involve the correlation and consolidation of data related to the same or apparently similar events.

4.3.6 Relevance

The organization shall ensure that all data are relevant, i.e. that the data collected meet the current and potential future needs of users in analysing and reporting, as well as taking action for as well as monitoring the safety of health software.

4.4 Process model

4.4.1 General

As indicated by the arc superimposed on Figure 1 below, the Recording, Analysing and Reporting data processes related to the safety of health software are the focus of this document. It is acknowledged that the additional steps involving Action as well as Monitoring and Review complete the incident data cycle, however, these are not part of the scope of this document.

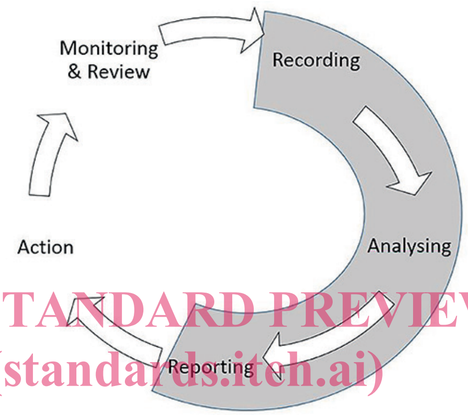

Figure 1 — Health software safety event management data cycle

4.4.2 Recording

The organization shall establish, document and maintain a process to collect data relating to health software safety events in a proactive fashion. Where possible, this shall be a coordinated process within the organization and, as possible, undertaken in the same or similar fashion to the framework with peer organizations.

4.4.3 Analysing

The organization shall establish, document and maintain processes to analyse data relating to health software safety events in a proactive fashion including but not limited to direct or indirect causative factors, contributing factors and other important aspects and influences. This analysis shall also assess the impact of any consequent or recurrent data related to the on-going validity of any analysis or report involving the safety of health software.

4.4.4 Reporting

The organization shall ensure that data and analysis related to health software safety events are reported in a timely manner. The organization should strive to ensure that reports are easy to use and understand and, as possible, are widely available to stakeholders and interests. As appropriate to improving the overall approach, and while safeguarding any personal health information, the original data as collected should be made available along with the report.