INTERNATIONAL STANDARD

ISO 29585

First edition
2023-06

Health informatics — Framework for healthcare and related data reporting

Reference number
ISO 29585:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of 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 www.iso.org/iso/foreword.html.

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

This first edition of ISO 29585 cancels and replaces ISO/TR 22221:2006 and ISO/TS 29585:2010, which have been technically revised.

The main changes are as follows:

— consideration of the impact of developments such as the availability of big-data and federation of services;

— each requirement has an identified actor responsible for its delivery and each requirement is intended to be clear and unambiguous.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

0.1 Background

A considerable amount of data is collected during the provision of care and treatment, some of it specific to the patient being treated, and some of it not. The primary purpose of this information is to support and improve individual patient care and much of it is held under professional and legal obligations of confidentiality. However, this information, often in conjunction with other records, is of value for many other purposes to support healthcare for groups of patients or for populations.

Healthcare data reporting provides many benefits. The health and well-being of the population are improved by activities such as disease surveillance, screening, needs assessment and preventative activities such as identifying the relationship between infected water and cholera resulting in better sewers. Research has led to major benefits in health practice such as the cure of duodenal ulcers, prevention of spina bifida, effective treatment of breast cancer and the carrying out of hip replacements. Research has also reduced risks through a greater understanding of HIV prevention, the relationship between smoking and lung cancer and the ill effects of the use of aspirin for children. The regulation of new medicines and other treatments relies on evidence of safety and efficacy from clinical trials.

Providing appropriate conditions are met, these data can legitimately be used to support these other purposes. In practice, such healthcare data reporting covers a wide spectrum including:

— Protecting the health of the public through surveillance and immediate response to infectious disease and other environmental threats to health, monitoring adverse effects of therapeutic interventions and informing and evaluating screening.

— Providing better information to the general public about healthy lifestyles.

— Improving the quality and safety of care or reducing the impact of new risks to population.

— Improving the management of the health system, for example by supporting the more efficient commissioning of services and value-based care.

— Improving the quality of clinical care within an institution, for example through the audit of clinical practice.

— Identifying patients who interact with multiple parts of the health system in order to monitor equity of access and provision:

  — ensuring consistent care for people who interact with multiple parts of the system,

  — monitoring equity of access and provision.

— Ensuring that health policy is evidence-based through carrying out empirical research.

0.2 Healthcare data reporting

Where the term "clinical data warehouse" implied a specific, bounded, repository of data, with specific functions, recent developments have greatly increased the ways of addressing potential applications. For instance:

— The era of "big data" offering new sources and modes of data, with a massive increase in data capture and use, including structured, unstructured, text, images, near real-time, combination of data sources, e.g. personal device data, also social determinant of health data to inform population health and a wide range of presentation and visualization tools.

— The establishment of federated services that can link data sources which previously could not be combined and, hence, supporting distributed queries. These federated approaches can support moving from hierarchical views of data to multi-layered and multi-dimensional approaches, the separation of data sources and data consumers, distributed queries and moving from data warehouses / data marts to data lakes and data labs.

— The potential for analysing data on a much wider scale, particularly for areas such as rare diseases where federated big data enables studies requiring this population size.

— The push for transparency of data has further reinforced the opportunities and responsibilities of sharing the value of such analysis with a wider public.

In view of these developments, this document provides a framework for healthcare and data reporting, addressing both the opportunities and the responsibilities of the handling of the data. Figure 1 summarizes the stages, products and actors through the lifecycle.

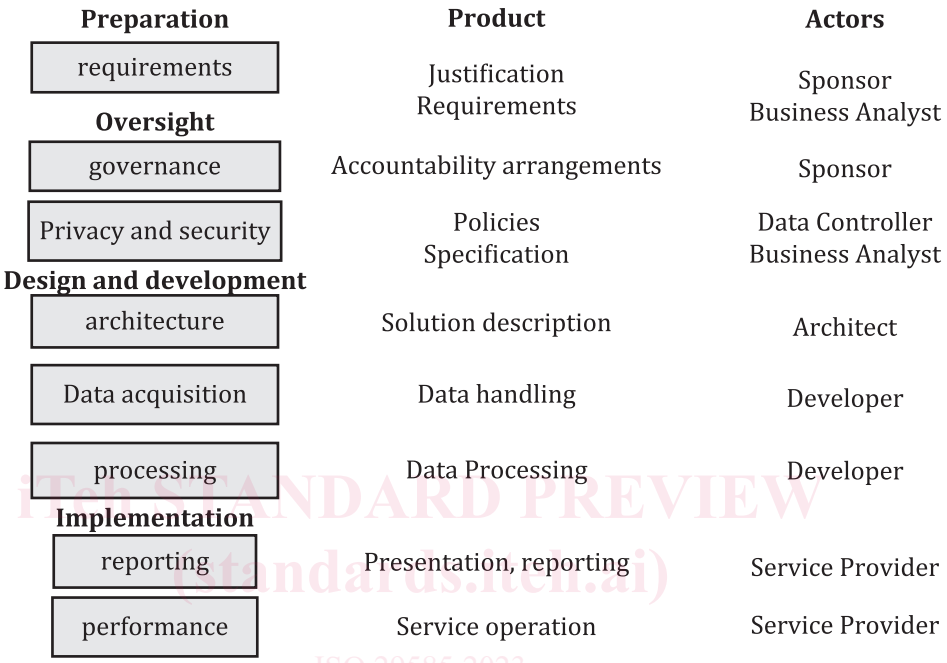

Figure 1 — Lifecycle for a healthcare data reporting service

Clauses 5 to 12 specify requirements, each of which is allocated to one actor. Requirements are individually referenced by actor (e.g. SPnnn for sponsor, DCnnn for data controller, ANnnn for business analyst, ARnnn for architect, DVnnn for developer and PRnnn for service provider).

Health informatics — Framework for healthcare and related data reporting

1 Scope

This document deals with the reporting of data to support improved public health, more effective health care and better health outcomes.

This document provides guidance and requirements for those developing or deploying a healthcare data reporting service, addressing data capture, processing, aggregation and data modelling and architecture and technology approaches.

The role of a healthcare data reporting service is to enable data analyses in support of effective policies and decision making, to improve quality of care, to improve health services organizations and to influence learning and research. This document has relevance to both developing and more established health systems. It enables meaningful comparison of programs and outcomes.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62304, *Medical device software — Software life cycle processes*

3 Terms and definitions

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

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

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

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

3.1
analyst
member of the technical community who is skilled and trained to define problems and to analyze, develop, and express algorithms

EXAMPLE Systems engineer, business analyst.

3.2
architect
person, team, or organization responsible for the process of defining a collection of hardware and software components and their interfaces to establish the framework for the development of a computer system

[SOURCE: ISO/IEC/IEEE 24765:2017, modified — Combined definitions of "architect" (3.209) and "architectural design" (3.211).]

3.3
business analyst
person who bridges the gap of understanding between business and technology to accurately define software requirements and carefully control scope

3.4
clinical data warehouse
CDW
grouping of data accessible by a single data management system, possibly of diverse sources, pertaining to a health system or sub-system and enabling secondary data analysis for questions relevant to understanding the functioning of that health system, and hence supporting proper maintenance and improvement of that health system, e.g. public health services

Note 1 to entry: A CDW tends not to be used in real time. However, depending on the rapidity of transfer of data to the data warehouse, and data integrity, near real-time applications are not excluded.

3.5
dashboard
user interface based on predetermined reports, indicators and data fields, upon which the end user can apply filters and graphical display methods to answer predetermined business questions and which is suited to regular use with minimal training

3.6
data controller
organization that determines what information will be processed and why

Note 1 to entry: The data processor is the one that does the actual processing. Controllers are responsible for creating privacy notices, implementing mechanisms to ensure that individuals can exercise their data subject rights and adopting measures to ensure the data processing meets the GDPR's (general data protection regulation) principle of privacy by design and by default.

3.7
data custodian
role within the processing entity (IT department) that handles the data daily

3.8
data dictionary
database used for data that refer to the use and structure of other data, i.e. a database for the storage of metadata

3.9
data element
unit of data that is considered in context to be indivisible

3.10
data mart
subject area of interest within or standalone from the data warehouse dimension

EXAMPLE An inpatient data mart.

Note 1 to entry: Data marts can also exist as a standalone database tuned for query and analysis, independent of a data warehouse.

Note 2 to entry: Data marts are typically suitable to adhere to localized requirements such as GDPR (general data protection regulation) in the European Union, via clear specification of purpose for analysis, permissions of data subjects, and data minimalization procedures.

3.11
data warehouse dimension
subject-oriented, often hierarchical business relevant grouping of data

3.12
developer
individual or organization that performs development activities (including requirements analysis, design, testing through acceptance) during the system or software life-cycle process

[SOURCE: ISO/IEC 25000:2014, 4.6]

3.13
drill down
exploration of multidimensional data which makes it possible to move down from one level of detail to a more detailed level depending on the granularity of data

EXAMPLE Number of patients by departments and/or by services.

3.14
episode of care
identifiable grouping of healthcare-related activities characterized by the entity relationship between the subject of care and a healthcare provider, such grouping determined by the healthcare provider

3.15
health indicator
single summary measure, most often expressed in quantitative terms, that represents a key dimension of health status, the healthcare system, or related factors

Note 1 to entry: A health indicator is informative and also sensitive to variations over time and across jurisdictions.

[SOURCE: ISO 21667:2010, 2.2]

3.16
healthcare data reporting service
managed service to provide reporting of data to support improved public health, more effective health care and better health outcomes

3.17
metadata
information stored in the data dictionary that describes the content of a document

3.18
master data management
enablement of a program that provides for an organization's data definitions, source locations, ownership and maintenance rules

3.19
organization
unique framework of authority within which a person or persons act, or are designated to act towards some purpose

[SOURCE: ISO/IEC 6523-1:1998, 3.1, modified — Removed note to entry.]

3.20
performance indicator
measure that supports the evaluation of an aspect of performance and its change over time

3.21
service provider
organization or part of an organization that manages and delivers a service or services to the customer

Note 1 to entry: A customer can be internal or external to the service provider's organization.

3.22
sponsor
person or group who provides resources and support for the project, program, or portfolio and is accountable for enabling success

[SOURCE: ISO/IEC TR 24587:2021, 3.15]

3.23
star schema
dimensional modelling concept that refers to a collection of fact and dimension tables

4 Abbreviated terms

AES	Advanced Encryption Standard
API	Application Programming Interface
DPO	Data Protection Officer
EHR	Electronic Health Record
ELT	Extract, Load, Transform
ETL	Extract, Transform, Load
GDPR	General Data Protection Regulation
HL7®[a)]	Health Level 7
ICD®[b)]	International Classification of Diseases
LOINC®[c)]	Logical Observation Identifiers, Names and Codes
MBUN	Meaningless But Unique Number
NLP	Natural Language Processing
OCR	Optical Character Recognition
PIA	Privacy Impact Assessment [020 – amended]
RBAC	Role-based Access Control
SLA	Service Level Agreement
SNOMED CT®[d)]	Systematized Nomenclature of Medicine — Clinical Terms
TRE	Trusted Research Environment

[a] HL7 is the registered trademark of Health Level Seven International. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named.

[b] ICD is the trademark of the WHO. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named.

[c] LOINC is the registered trademark of Regenstrief Institute. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named.

[d] SNOMED CT is the registered trademark of the International Health Terminology Standards Development Organisation (IHTSDO). This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named.

5 Preparing: Requirements and planning

5.1 Overview

Clause 5 describes steps to be taken when planning the development of healthcare data reporting service or the extension of existing services. Potential benefits and uses are described in Annex A.

The sponsor and the business analyst are responsible for specifying requirements.

A healthcare data reporting service typically becomes more valued than originally anticipated and grow in size, complexity and rate of access.

SP001 The sponsor should ensure that the healthcare data reporting service be viewed as an on-going development and not as a fixed project with an endpoint.

SP002 The sponsor should provide an “extensibility” plan can include import and export to other systems and communications with other systems, which retain the integrity of the data.

5.2 Prioritization of requirements

There are many factors relevant to the prioritization of requirements.

SP003 A sponsor wishing to develop, extend or make use of the healthcare data reporting service should justify the purposes of use prior to commencing implementation.

SP004 The sponsor shall have a clear value proposition for the foreseen applications.

SP005 The sponsor should, when developing new services, include engagement with initial information providers, users, service providers and other relevant systems with which the healthcare data reporting service is expected to exchange information/services.

SP006 The sponsor shall ensure that proposals are designed to achieve a clear outcome for users or the system. The sponsor shall understand how outputs will result in better provision and/or outcomes for people and the health and care system.

SP007 The sponsor shall document the justification for the intended purpose(s) of the healthcare data reporting service.

SP008 The sponsor should ensure budgets balance costs and performance needs.

SP009 The sponsor can enter into contractual requirements for the healthcare data reporting service with current information systems and service suppliers.

SP010 The sponsor of the healthcare data reporting service shall ensure that the service is scalable.

5.3 Users

Consideration should be given to multiple levels of reporting, such as national, regional, local and international.

Commercial users, government entities, regulators, professional bodies and educational establishments can exist in some form at all levels.

Level	Example
International	agencies such as the World Health Organization (WHO), research bodies such as the Commonwealth Fund or groupings such as the European Union
	governments, government agencies (e.g. analysis and reporting centres), regulators, professional bodies, universities, medical research
Regional	depending on the country, can be state, province or regional government, or health organizations
Local	local care organizations (e.g. health care providers or hospitals), local government for environment, education, housing, other commercial users, e.g. pharmaceutical companies

It is often appropriate to have reporting at each of these levels, each attuned to the analysis and reporting requirements of the sponsoring organization.

SP011 The sponsor should ensure the healthcare data reporting service provides policy and strategic reporting to meet the needs of the stakeholders.

SP012 The sponsor should ensure the healthcare data reporting service has the ability to support day-to-day requirements for the intended stakeholders.

5.4 Data requirements

SP013 The sponsor of the healthcare data reporting service shall ensure that the service has availability of data and corresponding metadata from source systems.

SP014 The sponsor of the healthcare data reporting service shall ensure that the service includes data quality measures that reflect fitness for purpose.

SP015 The sponsor shall document a structured process that reviews current and planned arrangements for handling of personal data.

SP016 The sponsor shall identify, establish and use standards for handling health data.

SP017 The sponsor shall demonstrate that the product collects, stores and processes users' information in a safe and fair way, the handling of personal information.

5.5 Services and non-functional requirements

Provisioning through cloud-based services places more emphasis on supplier and consumer relationships. All the following features are important for the effectiveness of any reporting, based on agreed measures and metrics

SP018 The sponsor of the healthcare data reporting service shall ensure that the service is provided with appropriate Service Level Agreements, or equivalent, regarding ongoing technical support with suitable availability from a helpdesk or similar.

SP019 The sponsor of the healthcare data reporting service shall ensure that the service perform periodic backups and test restores as specified by Service Level Agreements (SLA).

SP020 The sponsor of the healthcare data reporting service shall ensure that the service has a plan for disaster recovery.

SP021 The sponsor shall ensure services are reviewed at least annually to identify and improve processes, which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

SP022 The sponsor of the healthcare data reporting service shall ensure that the service accommodate the highly dimensional and complex nature of healthcare data and associated analysis

SP023 The sponsor shall ensure that the data requirements take account of the types of output through which the data will be reported.

SP024 The sponsor should ensure that the development of outputs for clinical use involves both technical and clinical expertise in the form of a clinical product owner.

6 Governance

6.1 Principles

Clause 6 considers the governance issues of responsible data organization, management and use.

The primary actors in this clause are the sponsor and, in the context of guarding data access, the data custodian.

SP025 The sponsor shall define a governing structure for establishing policies and decision-making process regarding scope, access, further development, etc.

SP026 The sponsor shall base governance on data protection principles appropriate to country(ies) of operation.

SP027 The sponsor shall ensure there is a risk assessment and control system in place.

SP028 The sponsor shall ensure that governance arrangements include conformity with mechanisms for assuring that all plans have been completed and actions undertaken satisfactorily. Relevant International Standards for data governance include ISO/IEC 38505-1.

SP029 The sponsor shall ensure proposals are reviewed by an appropriate independent body (e.g. ethics committee).

SP030 The sponsor shall identify who is responsible for creating and enforcing policies that specify how data should be managed, used and maintained.

SP031 The sponsor of the healthcare data reporting service shall ensure that the service has audit policies, based on information governance principles (e.g. to ensure no identifiable personal data is revealed to the service provider except where unavoidable, and then all such access should be recorded and processes in place to detect misuse).

SP032 The sponsor shall ensure that, as the healthcare data reporting service is considered a key system, it is included within an overall business continuity plan.

7 Privacy and security of the data

7.1 Overview

Clause 7 describes general considerations regarding privacy and security. It is based on the premise that, prior to consideration of the architecture, there needs to be detailed assessment and planning for addressing confidentiality of personal data, to enable and support privacy by design.

The primary actors responsible in this clause are the sponsor, the business analyst responsible for specifying requirements and the data controller responsible for safeguarding data access.

This document is not a security framework, but it is intended that, within this healthcare data reporting framework, there is a corresponding security framework. Examples include ISO/IEC 27000, NIST SP 800-53, NIST SP 800-171, NIST Cybersecurity Framework, CIS Controls, HITRUST CSF[13] and COBIT[14].

SP033 The sponsor of the healthcare data reporting service shall ensure that the service addresses privacy and security aspects.

7.2 Principles

The following principles underpin the privacy measures for the healthcare reporting service:

DC001 The data controller shall ensure that data are collected for specified, explicit and legitimate purposes.

DC002 The data controller shall ensure that data are not further processed in a manner that is incompatible with those purposes for which it was collected.

DC003 The data controller shall ensure that collected data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization").