TECHNICAL SPECIFICATION

ISO/TS 21089

First edition
2018-04

Health informatics — Trusted end-to-end information flows

Informatique de santé — Flux d'informations "trusted end-to-end"

Reference number
ISO/TS 21089:2018(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*.

This first edition of ISO/TS 21089 cancels and replaces ISO/TR 21089:2004, which has been technically revised.

The main changes compared to ISO/TR 21089:2004 are as follows:

— transition from Technical Report (informative) to Technical Specification (normative);

— close alignment with ISO/HL7 10781:2015 and its specified record lifecycle events;

— close alignment with HL7 Fast Health Interoperable Resources (FHIR), Standard for Trial Use, 3rd Edition (STU-3) (2017), including the FHIR Record Lifecycle Event Implementation Guide (RLE IG) and two FHIR Resources AuditEvent and Provenance. See http://www.hl7.org/FHIR;

— incorporation of twenty-seven (27) record lifecycle events compared to fifteen (15) in the first edition for more complete representation of end-to-end electronic health record management;

— comprehensive review and update of terms and definitions (Clause 3) to more completely specify the range of health record lifespan and lifecycle events.

Introduction

This document describes requirements for health data/record management including identity, accountability, provenance, authenticity, integrity, confidentiality, stewardship and interoperability and addresses specific needs of health and healthcare stakeholders, in particular the individual subject of care, the healthcare professional/caregiver, the healthcare provider organization, its business units and the broader care community.

The trusted end-to-end information flows described herein offer necessary criteria for standards developers and implementers of electronic health record and other record management systems, including standards for data at rest (during retention) and data in motion (during exchange) within the healthcare domain and provide guidance for software developers and vendors, healthcare providers and end users.

Health informatics — Trusted end-to-end information flows

1 Scope

This document describes trusted end-to-end flow for health information and health data/record management. Health data is originated and retained, typically as discrete record entries within a trusted electronic health record (EHR), personal health record (PHR) or other system/device. Health data can include clinical genomics information.

Health record entries have a lifespan (period of time managed by one or more systems) and within that lifespan, various lifecycle events starting with "originate/retain". Subsequent record lifecycle events may include "update", "attest", "disclose", "transmit", "receive", "access/view" and more.

A record entry instance is managed – over its lifespan – by the source system. If record entry content is exchanged, this instance may also be managed intact by one or more downstream systems. Consistent, trusted management of record entry instances is the objective of this document, continuously and consistently whether the instance is at rest or in motion, before/during/after each lifecycle event, across one or more systems.

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 https://www.iso.org/obp

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

3.1
access, verb
obtain, open, inspect, review and/or make use of health data or information

Note 1 to entry: Access/View Record Lifecycle Event - occurs when an agent causes the system to obtain and open a record entry for inspection or review.

Note 2 to entry: See view (3.156).

[SOURCE: CPRI, modified]

3.2
access control
means of ensuring that the resources of an electronic system can be accessed only by authorized entities in authorized ways

Note 1 to entry: Alternatively, prevention of an unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

[SOURCE: ISO/IEC 2382-8:1998, modified]