
Health informatics — Trusted end-to-end information flows

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/TS 21089:2018](https://standards.iteh.ai/catalog/standards/sist/9d9297b5-0f4c-4b73-846f-00e2d94615f9/iso-ts-21089-2018)

<https://standards.iteh.ai/catalog/standards/sist/9d9297b5-0f4c-4b73-846f-00e2d94615f9/iso-ts-21089-2018>



iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/TS 21089:2018

<https://standards.iteh.ai/catalog/standards/sist/9d9297b5-0f4c-4b73-846f-00e2d94615f9/iso-ts-21089-2018>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	25
5 Truth, trust, end-to-end information flows and foundations of interoperability	27
6 Trust characteristics in end-to-end information flow	28
7 The trust constituency	29
8 Principles and objectives	32
8.1 Ensured trust	32
8.2 Trust constituency	32
8.3 Health record rights	33
8.4 Health record obligations	33
8.5 Health record composition	34
8.6 Human and business agents and their accountable actions	34
8.7 Software and device agents and their accountable actions	34
8.8 Scope of accountability	34
8.9 Provenance	35
8.10 Authentication	35
8.11 Auditability	36
8.12 Chain of trust	36
8.13 Faithfulness, permanence, persistence and indelibility	36
8.14 Data definition, data registry	36
8.15 Data integrity	36
8.16 Completeness	36
9 Downstream/upstream information flow perspectives	37
9.1 Downstream information flow perspective — Subject of care	37
9.2 Downstream information flow perspective — Accountable agent(s) for health record content	38
9.3 Upstream perspective — Accountable agent(s) for health record access/view	39
10 Agents, actions and corresponding persistent record entries	39
10.1 Agent takes action	39
10.2 Agent documents action taken	40
10.3 Agent stewards the record entry	40
11 Key contexts for action instances and record entry instances	41
11.1 Identity Context	41
11.2 Accountability Context	41
11.3 Data Integrity Context	41
11.4 Clinical Context	41
11.5 Administrative/operational context	42
12 Roles and relationships (examples)	42
12.1 Subject of care and provider relationships	42
12.2 Health services	42
12.3 Health record relationships	42
12.4 Individuals, organizations and business unit relationships	43
12.5 Inter-healthcare professional relationships	43
13 Record lifecycle events and CRUD (create, read, update, delete)	44

14	Key lifecycle events in trusted end-to-end information flows	46
15	Record lifecycle events and action instances	47
15.1	Initial instance	47
15.1.1	Initial action instance	47
15.1.2	Record lifecycle event — Originate/retain record entry instance(s)	48
15.2	Subsequent instance	50
15.2.1	Subsequent action instance	50
15.2.2	Record lifecycle event — Amend (update) record entry instance(s)	50
15.3	Record lifecycle event — Transform/translate	51
15.4	Record lifecycle event — Attest	52
15.5	Record lifecycle event — Access/view	53
15.6	Record lifecycle event — Report (output)	54
15.7	Record lifecycle event — Disclose	54
15.8	Record lifecycle event — Transmit	54
15.9	Record lifecycle event — Receive/retain	56
15.10	Record lifecycle event — De-identify (anonymize)	57
15.11	Record lifecycle event — Pseudonymize	58
15.12	Record lifecycle event — Re-identify	60
15.13	Record lifecycle event — Extract	61
15.14	Record lifecycle event — Archive	62
15.15	Record lifecycle event — Restore (from archive)	63
15.16	Record lifecycle event — Destroy/delete	64
15.17	Record lifecycle event — Deprecate	65
15.18	Record lifecycle event — Reactivate (from delete or deprecate)	66
15.19	Record lifecycle event — Merge	67
15.20	Record lifecycle event — Unmerge	68
15.21	Record lifecycle event — Link	69
15.22	Record lifecycle event — Unlink	69
15.23	Record lifecycle event — Add legal hold	70
15.24	Record lifecycle event — Remove legal hold	71
15.25	Record lifecycle event — Verify	72
15.26	Record lifecycle event — Encrypt	73
15.27	Record lifecycle event — Decrypt	74
	Annex A (informative) HL7 Fast Health Interoperable Resources (FHIR)	76
	Annex B (informative) Lifecycle metadata captured in FHIR resources	78
	Annex C (informative) Sample lifecycle event sequence with FHIR resources	82
	Annex D (informative) Lifecycle Event Sequence — Point of Origination to Point of Access (Example)	84
	Bibliography	85

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 21089:2018 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.

iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/TS 21089:2018

<https://standards.iteh.ai/catalog/standards/sist/9d9297b5-0f4c-4b73-846f-00e2d94615f9/iso-ts-21089-2018>

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]

3.3.1

accountability

obligation of an individual or organization to account for its activities, for completion of a deliverable or task, accept responsibility for those activities, deliverables or tasks, and to disclose the results in a transparent manner

3.3.2

accountability

<uniquely traceable> property that ensures that the actions of an entity can be traced uniquely to the entity

[SOURCE: ISO 7498-2:1998, 3.3.3, modified]

3.4

accuracy

<data> extent that recorded data reflect the actual underlying information

3.5

actor

with respect to an action, entity that participates in or observes that action

[SOURCE: ISO/IEC 15414:2015, modified]

3.6.1

agent

<conscious> entity that takes conscious actions, such as an individual, organization, business unit

3.6.2

agent

<delegated> entity that has been delegated (e.g. authority, a function) by and acts for another (in exercising the authority, performing the function)

<https://standards.iteh.ai/catalog/standards/sist/9d9297b5-0f4c-4b73-846f-00e2d94615f9/iso-ts-21089-2018>

3.6.3

agent

<healthcare> individual, organization, business unit, medical device (e.g. instrument, monitor) and software (e.g. application) which a) performs a role in the provision of healthcare services and/or b) is accountable for actions related to, and/or c) ascribed in, the health record

[SOURCE: CEN 12265:2014, modified]

3.6.4

agent

<programmed> entity that takes programmed actions, such as software or a device

3.6.5

agent

<responsible> entity that bears some form of responsibility for an activity taking place, for the existence of an entity, or for another agent's activity

3.7

aggregation

process to combine standardized data and information

[SOURCE: JCAHO, modified]

3.8.1

algorithm

<calculation/problem solving> process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer

3.8.2**algorithm**

<step-wise progression> series of steps for addressing a specific issue

[SOURCE: JCAHO, modified]

3.9**amend**

make changes in record content in order to make it fairer, more accurate, consistent, complete and/or up-to-date

Note 1 to entry: Amend (Update) Record Lifecycle Event - occurs when an agent makes any change to record entry content currently residing in storage considered permanent (persistent).

3.10**append**

add information as an attachment or supplement to a previous record entry instance or object already in existence

Note 1 to entry: It may be an attachment or supplement.

[SOURCE: HL7 RBAC, modified]

3.11**anonymize**

remove personally identifying particulars or characteristics from record content so that the original source or data subject cannot be known

Note 1 to entry: Anonymization is a sub-class of de-identification which is irreversible.

3.12**anonymous**

anonymized

unnamed or unidentified

ISO/TS 21089:2018

<https://standards.iteh.ai/catalog/standards/sist/9d9297b5-0f4c-4b73-846f-00e2d94615f9/iso-ts-21089-2018>

Note 1 to entry: It can include an unknown source or subject.

3.13**application**

identifiable computer running a software process

Note 1 to entry: In this context, it may be any software process used in healthcare information systems including those without any direct role in treatment or diagnosis.

Note 2 to entry: In some jurisdictions, software processes can be incorporated in regulated medical devices.

3.14**architecture**

set of principles on which the logical structure and interrelationships to an organization and business context are based

Note 1 to entry: Software architecture is the result of software design activity.

3.15**archive, verb**

create, update or move an archive artifact with health record content for long-term, typically offline storage, external to the source system

Note 1 to entry: Archive Record Lifecycle Event - occurs when an agent causes the system to create and move archive artifacts containing record entry content, typically to long-term offline storage.

Note 2 to entry: Also, to store data by moving it to long-term storage media and deleting or purging that data from the original online storage.

3.16

archival record

item of healthcare data saved for later reference or use, possibly off-line

[SOURCE: COACH, modified]

3.17.1

assurance

<surety> grounds for surety, certainty or confidence about something

[SOURCE: ISO/IEC 15408-1:2009, 3.1.4, modified]

3.17.2

assurance

<security> grounds for confidence that an entity meets its claimed level of protection, including security objectives

[SOURCE: OMG, modified]

3.17.3

assurance

<system services> development, documentation, testing, procedural and operational activities carried out to ensure a system's services do in fact provide the claimed level of function, performance and usability

[SOURCE: OMG, modified]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.18.1

attest

<authenticity/accuracy> declare that record entry content exists, is authentic, accurate and true and therefore that it can be trusted

[ISO/TS 21089:2018](https://standards.iteh.ai/catalog/standards/sist/9d9297b5-0f4c-4b73-846f-00e2d94615f9/iso-ts-21089-2018)

<https://standards.iteh.ai/catalog/standards/sist/9d9297b5-0f4c-4b73-846f-00e2d94615f9/iso-ts-21089-2018>

3.18.2

attest

<completion> declare that record entry content exists and is complete for the purpose intended

3.18.3

attest

<evidentiary> provide or serve as clear evidence of and thus certify and record applicable administrative (or "legal") responsibility for a particular unit of information

Note 1 to entry: Attest Record Lifecycle Event - occurs when an agent causes the system to capture the agent's digital signature (or equivalent indication) during formal validation of record entry content.

3.19

audit, noun

audit control

mechanism employed to record and examine activities of an agent

3.20

audit, noun

<security> independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures

3.21.1

audit trail

audit log

<evidence of resource utilization> record of the resources which were accessed and/or used by whom

[SOURCE: ISO 7498-2:1998, modified]

3.21.2**audit trail**

<evidence of information operations> documentary evidence of monitoring each operation (of healthcare parties) on health information

[SOURCE: NRC, modified]

3.21.3**audit trail**

<evidence of system use/activities> chronological record of system activities that is sufficient to enable the reconstruction, reviewing and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results

[SOURCE: GCST]

3.22**authentic**

<object> what it purports to be

Note 1 to entry: Also, genuine and of undisputed origin; bona fide; based on facts, accurate and reliable.

3.23.1**authentication**

process proving something is real, true, or genuine

3.23.2**authentication**

<data> process of verification of the integrity of data that have been captured, stored or transmitted

[SOURCE: GCST]

3.23.3**authentication**

<data source> process of corroboration that the source of data received is as claimed

3.23.4**authentication**

<identity of entity> process to provide assurance regarding the claimed identity of an entity (e.g. subject, user, author)

[SOURCE: ISO/IEC 10181-2:1996, 3.3, modified]

3.23.5**authentication**

<health record entries> process to verify that an entry exists, is complete, accurate and final

[SOURCE: JCAHO, modified]

3.23.6**authentication**

<object> process to assure the identity of an object

[SOURCE: ASTM E1762: 2013, modified]

3.24**authorize**

grant rights, which includes granting access based on access rights

[SOURCE: ISO 7498-2:1998, 3.3.10, modified]

3.25

authorization

prescription that a particular behaviour must not be prevented

[SOURCE: ISO/IEC 15414:2015]

3.26

authorized user

user who may, in accordance with a security policy, perform an operation

3.27.1

availability

<accessibility/usability> property of being accessible and useable upon demand by an authorized entity

[SOURCE: ISO 7498 2:1998]

3.27.2

availability

<non-concealment> prevention of the unauthorized withholding of information or resources

[SOURCE: ITSEC]

3.28

business unit

discrete and accountable function or sub-function within an organization

Note 1 to entry: A business unit can include a department, service or specialty within a healthcare provider organization.

3.29

care

provision of accommodations, comfort and treatment to an individual subject of care (patient)

[SOURCE: JCAHO]

3.30

caregiver

individual who is entrusted with the direct or indirect provision of defined healthcare services to an individual subject of care or to populations

Note 1 to entry: cf. healthcare professional ([3.71.1](#)).

3.31

clinical information

information about a subject of care, relevant to the health or treatment of that subject of care, that is recorded by or on behalf of a healthcare person

Note 1 to entry: Also, information related to the health and healthcare of an individual collected from or about an individual receiving healthcare services: includes a caregiver's objective measurement or subjective evaluation of a patient's physical or mental state of health, descriptions of an individual's health history and family health history, diagnostic studies, decision rationale, descriptions of procedures performed, findings, therapeutic interventions, medication prescribed; description of responses to treatment, prognostic statements, and descriptions of socio-economic and environmental factors related to the patient's health.

[SOURCE: CEN 1613:1994]

3.32

code set

group of keys or indices used for encoding data elements, such as tables of terms, medical concepts (e.g., medical diagnostic codes or medical procedure codes)

3.33 coding scheme

collection of rules that maps the elements of one set on to the elements of a second set

3.34 complete health record

final, assembled and authenticated, health record for an individual

Note 1 to entry: A health record is complete when a) its contents reflect the diagnosis, results of diagnostic tests, therapy rendered, condition and progress (of the subject of care), and condition (of the subject of care) at discharge, and b) its contents, including any required clinical résumé or final progress notes, are assembled and authenticated, and all final diagnoses and any complications are recorded without use of symbols or abbreviations.

[SOURCE: JCAHO]

3.35 completeness

extent to which relevant records are present and the fields in each record are populated appropriately

3.36.1 confidentiality

<controlled release> condition in which information is shared or released in a controlled manner

[SOURCE: NRC]

3.36.2 confidentiality

<labeling> status accorded to data or information indicating that it is sensitive for some reason, and that therefore it needs to be protected against theft or improper use and must be disseminated only to individuals or organizations authorized to have it

[SOURCE: OTA]

<https://standards.iteh.ai/catalog/standards/sist/9d9297b5-0f4c-4b73-846f-00e2d94615f9/iso-ts-21089-2018>

3.36.3 confidentiality

<need to know> restriction of access to data and information to individuals who have a need, a reason and permission for access

[SOURCE: JCAHO]

3.36.4 confidentiality

<not disclosed> property that information is not made available or disclosed to unauthorized individuals, entities or processes

[SOURCE: ISO 7498-2:1998, 3.3.16]

3.37.1 consent

<permission> voluntary agreement with what is being done or proposed (express or implied)

[SOURCE: CIHI]

3.37.2 consent

<dialogue> process of communication or correspondence between the caregiver and the subject of care

[SOURCE: CPRI, modified]

Note 1 to entry: May refer to consent for treatment, special procedures, release of information and/or advance directives (which give instructions regarding the subject of care's wishes in special medical situations).

3.38

continuity of care

component of patient care quality consisting of the degree to which the care needed by a patient is coordinated among practitioners and across organizations and time

3.39

constituency

class of persons served in common

Note 1 to entry: Typically a group of individuals and/or organizations with explicit common interests and who can elect or otherwise designate agents or delegates to represent such interests.

3.40

correct, verb

identify and remedy an error or inaccuracy in record content

Note 1 to entry: cf. amend (3.9).

3.41.1

credentials

<identity> data that are transferred to establish the claimed identity of an entity

[SOURCE: ISO/IEC 2382:2015]

3.41.2

credentials

<healthcare practice> documented evidence of (a healthcare professional's) licensure, education, training, experience, or other qualifications

[SOURCE: JCAHO]

3.42

criteria

expected level(s) of achievement, or specifications against which performance can be assessed

[SOURCE: JCAHO]

3.43

data

<healthcare> information elements which are input, stored, processed or output by the automated information system which support the clinical and business functions of a healthcare organization

Note 1 to entry: These data may relate to person identifiable records or may be part of an administrative system where persons are not identified.

[SOURCE: HL7, modified]

3.44

data attribute

data element

data item

single unit of data that in a certain context is considered indivisible

3.45

data consistency

for the uses intended, subject (data) elements that are clear and well defined enough to yield similar results in similar analyses

3.46.1**data integrity**

<non-alteration> property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 7498-2:1998]

3.46.2**data integrity**

<wholeness> accuracy, consistency and completeness of data/record content

[SOURCE: JCAHO, modified]

3.47**data reliability**

for the uses intended, subject (data) elements that demonstrate accuracy, completeness, integrity, stability, repeatability and precision

[SOURCE: JCAHO, modified]

3.48**data transmission**

sending of data or information from one location to another location; exchange of data between person and program, or program and program, when the sender and receiver are remote from each other

[SOURCE: JCAHO; CPRI]

3.49**data validity**

verification of correctness (reflecting the true situation)

Note 1 to entry: cf. validate (3.154).

[SOURCE: JCAHO] <https://standards.itech.ai/catalog/standards/sist/9d9297b5-0f4c-4b73-846f-00e2d94615f9/iso-ts-21089-2018>

3.50**decrypt**

decode or render information readable by algorithmically transforming ciphertext into plaintext

Note 1 to entry: Decrypt Record Lifecycle Event - occurs when an agent causes the system to decode record entry content from a cipher.

[SOURCE: HL7 ActCode code system, HL7 v3 ObligationPolicy value set, modified]

3.51**de-identify**

<disassociation> reduce the association between a set of identifying data and the data subject in a way that may or may not be reversible

Note 1 to entry: De-Identify (Anonymize) Record Lifecycle Event - occurs when an agent causes the system to scrub record entry content to reduce the association between a set of identifying data and the data subject in a way that may or may not be reversible.

Note 2 to entry: Also, remove all information which can be used to identify an individual where there is no reasonable basis to believe that the information left can be used to identify the individual.

[SOURCE: US HIPAA, modified]

3.52**delegate**

give authority, function, or responsibility to another

[SOURCE: ISO/IEC 15414:2015, modified]