

---

---

## Health informatics — Trusted end-to-end information flows

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



## **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](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

|  |           |
|--|-----------|
| <b>Foreword</b>  | <b>v</b>  |
| <b>Introduction</b>  | <b>vi</b> |
| <b>1 Scope</b>   | <b>1</b>  |
| <b>2 Normative references</b>  | <b>1</b>  |
| <b>3 Terms and definitions</b>   | <b>1</b>  |
| <b>4 Abbreviated terms</b>   | <b>25</b> |
| <b>5 Truth, trust, end-to-end information flows and foundations of interoperability</b>      | <b>27</b> |
| <b>6 Trust characteristics in end-to-end information flow</b>                                | <b>28</b> |
| <b>7 The trust constituency</b>  | <b>29</b> |
| <b>8 Principles and objectives</b>   | <b>32</b> |
| 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        |
| <b>9 Downstream/upstream information flow perspectives</b>                                   | <b>37</b> |
| 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        |
| <b>10 Agents, actions and corresponding persistent record entries</b>                        | <b>39</b> |
| 10.1 Agent takes action  | 39        |
| 10.2 Agent documents action taken  | 40        |
| 10.3 Agent stewards the record entry   | 40        |
| <b>11 Key contexts for action instances and record entry instances</b>                       | <b>41</b> |
| 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        |
| <b>12 Roles and relationships (examples)</b>   | <b>42</b> |
| 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        |
| <b>13 Record lifecycle events and CRUD (create, read, update, delete)</b>                    | <b>44</b> |

|           |   |           |
|-----------|---|-----------|
| <b>14</b> | <b>Key lifecycle events in trusted end-to-end information flows</b>                                       | <b>46</b> |
| <b>15</b> | <b>Record lifecycle events and action instances</b>   | <b>47</b> |
| 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        |
|           | <b>Annex A (informative) HL7 Fast Health Interoperable Resources (FHIR)</b>                               | <b>76</b> |
|           | <b>Annex B (informative) Lifecycle metadata captured in FHIR resources</b>                                | <b>78</b> |
|           | <b>Annex C (informative) Sample lifecycle event sequence with FHIR resources</b>                          | <b>82</b> |
|           | <b>Annex D (informative) Lifecycle Event Sequence — Point of Origination to Point of Access (Example)</b> | <b>84</b> |
|           | <b>Bibliography</b>   | <b>85</b> |

## 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](http://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](http://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](http://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]