



BSI Standards Publication

Health informatics — Trusted end-to-end information flows

National foreword

This Published Document is the UK implementation of ISO/TS 21089:2018.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 95378 1

ICS 35.240.80

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2018.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

Health informatics — Trusted end-to-end information flows

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





COPYRIGHT PROTECTED DOCUMENT

© ISO 2018, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	24
5 Truth, trust, end-to-end information flows and foundations of interoperability	27
6 Trust characteristics in end-to-end information flow	27
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	49
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	59
15.13	Record lifecycle event — Extract	60
15.14	Record lifecycle event — Archive	61
15.15	Record lifecycle event — Restore (from archive)	62
15.16	Record lifecycle event — Destroy/delete	63
15.17	Record lifecycle event — Deprecate	64
15.18	Record lifecycle event — Reactivate (from delete or deprecate)	65
15.19	Record lifecycle event — Merge	66
15.20	Record lifecycle event — Unmerge	67
15.21	Record lifecycle event — Link	68
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 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]

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)

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

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]

3.18.1
attest

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

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]

Note 1 to entry: Also, implying responsibility for safety.

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]

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]

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]

3.53

deprecate

designate data/record content as obsolete, erroneous or untrustworthy, as indication against its future use

Note 1 to entry: Deprecate Record Lifecycle Event - occurs when an agent causes the system to tag record entry(ies) as obsolete, erroneous or untrustworthy, to warn against its future use.

3.54

destroy

purge or expunge data/record content stored in electronic or magnetic media, typically based on explicit criteria, so that it is completely unreadable and cannot be accessed or used

Note 1 to entry: Destroy/Delete Record Lifecycle Event - occurs when an agent causes the system to permanently erase record entry content from the system.

Note 2 to entry: It may otherwise make the data inaccessible to the application system by removing information about the object from memory or storage.

3.55

device

identifiable computer or software controlled apparatus or instrument that can be the holder of a private encipherment key

Note 1 to entry: Device in this context is any device used in healthcare information systems including those without any direct role in treatment or diagnosis.

Note 2 to entry: Includes the class of regulated medical devices that meet the above definition.

3.56

digital signature

data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source, signer and integrity of the data unit and protect against forgery

Note 1 to entry: This term is usually reserved for digital values or checksums calculated using asymmetric techniques, where only the originator of the message can generate the digital signature but many people can verify it.

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

3.57

disclose

release, transfer, provide access to, or divulge in any other manner information outside the entity holding the information

[SOURCE: US HIPAA]

Note 1 to entry: Disclose Record Lifecycle Event - occurs when an agent causes the system to release, transfer, provision access to, or otherwise divulge record entry content.

3.58

disclosure

<health information> release of information to third parties within or outside the healthcare provider organization from an individual's (health) record with or without the consent of the individual to whom the record pertains

[SOURCE: CPRI]

3.59

documentation

process of recording information in the (health) record

[SOURCE: JCAHO]

3.60

effectiveness

<of care> degree to which the care is provided in the correct manner, given the current state of knowledge, to achieve the desired or projected outcome for the (subject of care)

[SOURCE: JCAHO]

3.61

electronic health record

repository of (organized sets of) information regarding the health of a subject of care, in computer processable form

[SOURCE: ISO 20514:2015, modified]

3.62

encrypt

encode or render information unreadable by algorithmically transforming plaintext into ciphertext where data are temporarily re-arranged into an unreadable or unintelligible form for confidentiality, transmission, or other security purposes

[SOURCE: HL7 Version 3 Standard: Security and Privacy Ontology, Release 1, modified]

Note 1 to entry: Encrypt Record Lifecycle Event - occurs when an agent causes the system to encode record entry content in a cipher.

3.63

entity

physical, digital, conceptual, or other kind of thing with some fixed aspects, such as a person, body, or object

[SOURCE: W3C, modified]

3.64.1

evidence

<demonstrate truth> everything that is used to determine or demonstrate the truth of an assertion

3.64.2

evidence

<fulfill burden of proof> currency by which one fulfills the burden of proof

3.65

extract, verb

select, copy out or cite a set of health data/record content, typically based on explicit criteria

Note 1 to entry: Extract Record Lifecycle Event - occurs when an agent causes the system to selectively pull out a subset of record entry content, based on explicit criteria.

Note 2 to entry: Also, remove for separate consideration or publication.

3.66

health information

information, whether oral or recorded in any form or medium, that a) is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearing-house, and b) relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual

[SOURCE: HIPAA, modified]

3.67

health record

account compiled [by healthcare parties (physicians and other healthcare professionals)] of a variety of (subject of care) health information, such as (the subject of care's) assessment findings, treatment details and progress notes

[SOURCE: JCAHO, modified]

3.68

health/care

health and/or healthcare (in context)

3.69

healthcare

care, services, or supplies related to the health of an individual

[SOURCE: HIPAA]

Note 1 to entry: Includes any: a) preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counselling, service, or procedure with respect to the physical or mental condition, or functional status, of a patient or affecting the structure or function of the body; b) sale or dispensing of a drug, device, equipment, or other item pursuant to a prescription; or c) procurement or banking of blood, sperm, organs, or any other tissue for administration to patients.

3.70

healthcare informatics

scientific discipline that is concerned with the cognitive, information processing and communication tasks of healthcare practice, education and research, including the information science and technology to support these tasks

[SOURCE: Directory of the European Standardization Requirements for Healthcare Informatics and Telematics v2.1]

3.71.1

healthcare professional

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

3.71.2

healthcare professional

<qualification> person that is authorized by a nationally recognized body to be qualified to perform certain health services

Note 1 to entry: The types of registering or accrediting bodies differ in different countries and for different professions. Nationally recognized bodies include local or regional governmental agencies, independent professional associations and other formally and nationally recognized organizations. They may be exclusive or non-exclusive in their territory.

Note 2 to entry: Examples of health professionals are physicians, registered nurses and pharmacists.

[SOURCE: CEN 1613:1994, modified]

3.72

healthcare provider organization

healthcare institution responsible for the provision of healthcare to a subject of care or to a population

[SOURCE: CEN 13940:2000, modified]

3.73

health plan

individual or group program that provides, or pays the cost of, medical care

[SOURCE: HIPAA, modified]

3.74.1

identifier

<claimed> piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

[SOURCE: CEN ENV 13608-1:2005, modified]

3.74.2

identifier

<unique> identity information that unambiguously distinguishes one entity from another one in a given identity domain

3.75

indelible

impossible to remove or erase

3.76

indicator

<performance> measure used to determine over time (an organization's) accomplishment or fulfilment of functions, processes and outcomes

[SOURCE: JCAHO]

3.77

individually identifiable health information

information, including demographic information collected from an individual, that a) is created or received by a healthcare provider, health plan employer, or healthcare clearing-house; and b) relates to the past, present or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual, and i) identifies the individual, or ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual

[SOURCE: HIPAA]

3.78

information

interpreted set(s) of data that can assist in decision making; data to which meaning is assigned, according to context and assumed conventions

[SOURCE: JCAHO; NSC, modified]

3.79

integrity

<message> proof that the message content has not altered, deliberately or accidentally in any way, during transmission

Note 1 to entry: cf. data integrity (3.46).

[SOURCE: ISO/IEC 7498-2:1998]

3.80 **interface**

process that permits the flow of data/record content from one system to another in a structured manner

3.81.1 **interoperability**

<semantic> ability of different information technology systems and software applications to communicate, exchange data, and use the information that has been exchanged

3.81.2 **interoperability**

<standards-based> ability for data to be shared across clinicians, lab, hospital, pharmacy and patient, facilitated by data exchange schema and standards, regardless of the application or application vendor

Note 1 to entry: Also, ability of health information systems to work together within and across organizational boundaries in order to advance the health status of, and the effective delivery of healthcare for, individuals and communities.

[SOURCE: HIMSS, modified]

3.82 **legal hold** **litigation hold**

operation that tags or otherwise cues special access management and destruction suspension for Record Entries deemed relevant, consistent with organization policy under the legal doctrine of “duty to preserve”, also notifying records owners and other designated parties of the special data controls on access, retention, and destruction processes

Note 1 to entry: Add Legal Hold Record Lifecycle Event - occurs when an agent causes the system to tag or otherwise indicate special access management and suspension of record entry deletion/destruction, if deemed relevant to a lawsuit or which are reasonably anticipated to be relevant or to fulfill organizational policy under the legal doctrine of “duty to preserve”.

3.83 **legal hold removal** **legal hold release**

operation that untags or otherwise removes cues for special access management and destruction suspension for record entries as organization policy had required under the legal doctrine of “duty to preserve”, also notifying records owners and other designated parties of the release of special data controls and that the organization will resume normal data retention and destruction processes; provide notification to the records owners of the release of data and that the organization will resume normal data retention and destruction processes

Note 1 to entry: Remove Legal Hold Record Lifecycle Event - occurs when an agent causes the system to remove a tag or other cues for special access management had required to fulfill organizational policy under the legal doctrine of “duty to preserve”.

3.84 **lifecycle**

<record entry> stages during the lifespan of a health record entry instance

3.85 **lifecycle event**

<record entry> operation occurring during the course of record entry instance lifespan such as: originate, retain, amend (update), attest, exchange (transmit, receipt), access/view

3.86 **lifespan**

<record entry> period of time from the point of record entry instance origination to the point of record entry instance loss, destruction or deletion

3.87

link, verb

perform an operation that connects (establish a relationship between) two or more separate but related health records so that access or use of one necessarily means equal access to ability to use of all the connected records

Note 1 to entry: Link Record Lifecycle Event - occurs when an agent causes the system to connect related record entries.

3.88

longitudinal personal health record **lifetime personal health record**

permanent, coordinated record of significant information, in chronological sequence

Note 1 to entry: Also, may include all historical data collected or be retrieved as a user designated synopsis of significant demographic, genetic, clinical and environmental facts and events maintained within an automated system.

[SOURCE: ASTM E1384]

3.89

master file

dataset containing definitional entries in common across system, business units and, in some cases, organizational boundaries

Note 1 to entry: For example, master files may include data group and attribute definitions, security policy and domain definitions, security classification and clearance definitions, healthcare service definitions, care protocol definitions.

3.90

master patient index **MPI**

catalog within a given healthcare organization which serves as a directory to patients (subjects of care)

[SOURCE: CPRI, modified]

3.91

measure, verb

collect quantifiable data about a function or process

[SOURCE: JCAHO]

3.92

merge

<record entries> perform an operation that combines or joins the content of two or more health records, resulting in a single logical record entry

Note 1 to entry: Includes health records found to be registered as separate patients but are really one.

Note 2 to entry: Merge Record Lifecycle Event - occurs when an agent causes the system to combine or join content from two or more record entries, resulting in a single logical record entry.

3.93

message

logically ordered dataset designed to communicate essential information between systems

3.94

need-to-know

requirement for access to, knowledge, or possession of the classified information in order to perform tasks, functions or services

[SOURCE: ISO/IEC 2382:2015, modified]

3.95

network

electronic data transmission facility which can comprise just a point-to-point wire link between two devices, or a complex arrangement of transmission lines

3.96

non-repudiation

<of origination, of submission, of receipt> service that provides proof of the integrity and source of data (both in an unforgeable relationship) and that only the signer could have created the associated signature, which can be verified by any party

[SOURCE: ASTM E1762, modified]

3.97

organization

unique framework of authority within which a person or persons act, or are designated to act towards the same purpose

[SOURCE: ISO 6523:1998]

3.98

originate

<record entry> create or initiate an entry in a persistent datastore, such as an electronic or personal health record (EHR/PHR)

Note 1 to entry: Originate/Retain Record Lifecycle Event - occurs when an agent causes the system to: a) initiate capture of potential record content, and b) incorporate that content into the storage considered a permanent part of the health record.

3.99

output, verb

produce and deliver health record content in the form and manner expected by a viewer or recipient (e.g., printout, visual rendering, tagged or delimited data stream)

Note 1 to entry: cf. report ([3.126](#))

3.100

outcome

result of the performance (or non-performance) of a function or process(es)

Note 1 to entry: Also, condition or occurrence traceable to a cause.

[SOURCE: JCAHO, modified]

3.101

party

<object modeling> natural person or any other entity considered to have the same rights, powers and duties of a natural person

[SOURCE: ISO/IEC 15414:2015]

3.102

patient

person or defined groups of persons receiving or registered as eligible to receive healthcare services or having received healthcare services

Note 1 to entry: cf. subject of care ([3.139](#)).

3.103

patient safety

prevention of accidental or preventable injuries and mitigation of harm caused by errors of omission or commission that are associated with healthcare, and involving the establishment of operational systems and processes that minimize the likelihood of errors and maximize the likelihood of intercepting them when they occur

[SOURCE: NQF, modified]

3.104

performance

way in which an individual, group or organization carries out, accomplishes and fulfils its important functions and processes, usually with regard to effectiveness

[SOURCE: JCAHO, modified]

3.105

performance measure

standard or indicator, used to assess the capabilities of a function or process of any organization

Note 1 to entry: Also, quantification of processes and outcomes using one or more dimensions of performance, such as timeliness or availability.

[SOURCE: JCAHO]

3.106

persistent

existing or remaining in the same state for an indefinitely long time

3.107

personal health information

information that concerns a person's health, medical history, medical treatment or genetic characteristics in a form that enables the person to be identified

[SOURCE: MEDSEC]

3.108

personal information

information relating to an identified or identifiable natural person

[SOURCE: EU Directive 95/46/EC, MEDSEC]

3.109

policy

set of rules related to a particular purpose

[SOURCE: ISO/IEC 15414:2015]

Note 1 to entry: A rule can be expressed as an obligation, an authorization, a permission or a prohibition.

3.110

practice guidelines

descriptive tools or standardized specification for care of the typical subject of care in the typical situation, developed through a formal process that incorporates the best scientific evidence of effectiveness with expert opinion

[SOURCE: JCAHO]

3.111

primary record

records captured and maintained for the chief purpose of: a) supporting individual health and providing healthcare; b) clinical use including care, interventions and decision making

3.112.1

privacy

<information practices> security principle that protects individuals from the collection, storage and dissemination of information about themselves and the possible compromises resulting from unauthorized release of that information

[SOURCE: HL7]

3.112.2

privacy

<right> right of individuals to keep information about themselves from being disclosed to anyone

Note 1 to entry: Also, freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual and the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively.

[SOURCE: ISO/IEC 2382-8:2015, modified]

3.113

process

sequence of goal-directed, interrelated series of actions, events, mechanisms, or steps taking place in a prescribed manner and leading to the accomplishment of some result

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

3.114

protocol

<care> written plan specifying the procedures to be followed in giving a particular examination, conducting research, or providing care for a particular condition

3.115

pseudonymize

remove individually identifiable data/record content and replace with identity-bearing content for another entity

Note 1 to entry: Pseudonymize Record Lifecycle Event - occurs when an agent causes the system to remove record entry content to reduce the association between a set of identifying data and the data subject in a way that may be reversible.

3.116

pseudonymization

sub-class of de-identification which can be performed with or without the possibility of re-identifying the subject of the data/record content

[SOURCE: ISO 25237:2017]

3.117.1

purpose

<of use> context and conditions of data/record use at a specific point in time, and within a specific setting

[SOURCE: ASTM 1986:2013, modified]

3.117.2

purpose

<of a system> practical advantage or intended effect of the system

[SOURCE: ISO/IEC 15414:2015]

3.118

quality

character, characteristic or property of anything that makes it good or bad, commendable or reprehensible, thus the degree of excellence that a thing possesses

Note 1 to entry: Also, totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implied needs or fitness for use.

[SOURCE: JCAHO; CEN, modified]

3.119

quality improvement

approach to the continuous study and improvement of the processes of providing healthcare services to meet the needs of patients and others

[SOURCE: JCAHO]

3.120

re-activate

<record entry> recreate or restore full status to health records and their content from a previous state of deletion or deprecation

Note 1 to entry: Re-activate Record Lifecycle Event - occurs when an agent causes the system to recreate or restore full status to record entries previously deleted or deprecated.

3.121

receive

capture an exchange artifact (e.g., message or document) from an external system or entity; acquire data objects that exist elsewhere for potential inclusion in an EHR record

Note 1 to entry: Receive/Retain Record Lifecycle Event - occurs when an agent causes the system to

- a) initiate capture of data content from elsewhere, and
- b) incorporate that content into the storage considered a permanent part of the health record.

Note 2 to entry: cf. retain ([3.130](#)).

[SOURCE: HL7 EHR, Security, and Privacy Joint Vocabulary Alignment Project]

3.122.1

record entry

<evidentiary> persistent documentation, recording or evidence of facts, context, findings and observations, with associated supporting system data or metadata, regarding an action taken to support individual health or provide healthcare

3.122.2

record entry

<indivisible notation> semantically indivisible clinical statement which may be structurally large or small, but which loses meaning if broken up

3.122.3

record entry

<instance> discrete notation, recording instance or dataset in (EHR/PHR/other) system datastore, suitably attributed, which forms part of, or a whole, contribution to a health(care) record at one place and time

[SOURCE: ISO 18308:2011, modified]

3.123

registry

server capable of holding data for the systematic and continuous follow up of information objects maintained in accordance with specific rules

3.124

re-identify

restore information to data that would allow the identification of the source of the information or the information subject

[SOURCE: HL7 Version 3 Standard: Security and Privacy Ontology, Release 1]

Note 1 to entry: Re-identify Record Lifecycle Event - occurs when an agent causes the system to restore information to data that allows identification of information source and/or information subject.

3.125

release of information

disclosure of documents containing (subject of care-) identifiable information to a third party requestor

[SOURCE: CPRI]

3.126

report, verb

make or present an official or formal account or summary of

Note 1 to entry: Report (Output) Record Lifecycle Event - occurs when an agent causes the system to produce and deliver record entry content in a particular form and manner.

Note 2 to entry: cf. output ([3.99](#)).

3.127

report, noun

formal document that gives information about a particular subject

3.128

resource

<enterprise object modeling> entity which is essential to some behaviour and which requires allocation or may become unavailable because it is in use or used up

[SOURCE: ISO/IEC 15414:2015]

3.129

restore

<record entry> recreate record entries and their content from a previously created archive artefact

Note 1 to entry: Restore Record Lifecycle Event - occurs when an agent causes the system to recreate record entries and their content from a previous created archive artefact.

Note 2 to entry: Also, produce another object with the same content as one previously backed up (i.e., recreates a readily usable copy) or reinstate an information system back to an error-free and secure state from which normal operation can resume.

[SOURCE: HL7 Version 3 Standard: Security and Privacy Ontology, Release 1; HL7 Security Services Framework]

3.130

retain

<record entry> store and maintain (in a persistent datastore) health records after their point of origination, update, receipt, re-identification, restoration, decryption, etc.

Note 1 to entry: cf. originate/retain ([3.98](#)), receive/retain ([3.121](#)).

3.131

retention

maintenance and preservation of information in some form (e.g. paper, microfilm, or electronic storage) for a given period of time

[SOURCE: CPRI]

3.132.1

safety

<normative> quality of a product to meet applicable standards and practices for design, construction or manufacture

3.132.2

safety

<patient> prevention of accidental or preventable injuries and mitigation of harm caused by errors of omission or commission that are associated with healthcare, and involving the establishment of operational systems and processes that minimize the likelihood of errors and maximize the likelihood of intercepting them when they occur

Note 1 to entry: cf. patient safety ([3.103](#)).

3.132.3

safety

<perceived> users' level of comfort and perception of risk

3.133

secondary record

record that is derived from the primary record and contains selected data elements

[SOURCE: ASTM E1384:2013]

Note 1 to entry: Also, record that is derived/extracted from the primary record for specific purposes of use.

3.134.1

security

<data> combination of availability, confidentiality, integrity and accountability including protection of data from intentional, accidental or unintentional alteration or destruction, or copying or disclosure to unauthorized persons, whether in storage, processing, or transit

[SOURCE: CEN ENV 13608-1:2005; JCAHO; MEDSEC, modified]

3.134.2

security

<system safeguards> result of effective protection measures including safeguards for protection of information systems against software deficiencies, operating mistakes, or sabotage, against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document and counter such threats

[SOURCE: NSC; IOM, modified]

3.135.1

security policy

<information> set of laws, rules, and practices that regulate how an organization manages, protects and distributes sensitive information

[SOURCE: US DOD]

3.135.2

security policy

<system> plan or course of action adopted for providing computer security including a statement of information values, protection responsibilities and organization commitment for a system

[SOURCE: ISO/IEC 2382:2015; US OTA]