TECHNICAL REPORT

ISO/TR 18307

First edition
2001-12-15

Health informatics — Interoperability and compatibility in messaging and communication standards — Key characteristics

Informatique de santé —Interoperabilité et compatibilité avec les normes de messagerie et de communication — Caractéristiques

Reference number
ISO/TR 18307:2001(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this Technical Report may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 18307 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Health informatics — Interoperability and compatibility in messaging and communication standards — Key characteristics

1 Scope

This Technical Report describes a set of key characteristics to achieve interoperability and compatibility in trusted health information interchange between communicant application systems.

The key characteristics describe inter-application interoperability needs of the healthcare community, in particular the subject of care, the healthcare professional/caregiver, the healthcare provider organization, its business units and the integrated delivery network.

The key characteristics offer criteria for standards developers and implementers of standards for messaging and communications in the healthcare domain and provide a guide for software developers and vendors, healthcare providers and end users.

2 References

ISO/IEC Guide:1996, Guide 2: definition 3.2

ISO 2382-4, *Information technology — Vocabulary — Part 4: Organization of data*

ISO 6523-1:1998, *Information technology — Structure for the identification of organizations and organization parts — Part 1: Identification of organization identification schemes*

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

ISO/IEC 10746-2:1996, *Information technology — Open Distributed Processing — Reference Model: Foundations*

ISO/IEC 10746-3:1996, *Information technology — Open Distributed Processing — Reference Model: Architecture*

ISO/IEC 10746-4:1998, *Information technology — Open Distributed Processing — Reference Model: Architectural Semantics*

ISO/IEC 15408-1:1999, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

3 Terms and definitions

3.1
access
ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource

[HIPAA]

provision of an opportunity to approach, inspect, review, make use of data or information

[CPRI]

specific type of interaction between a subject and an object that results in the flow of information from one to the other

[GCST]

3.2
access control
means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways

[ISO/IEC 2382-8]

prevention of an unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner

[ISO 7498-2]

policies and procedures preventing access by those who are not authorized to have it

[IOM]

3.3
access level
level associated with an individual who may be accessing information (e.g. a clearance level)…, the information which may be accessed (e.g. a classification level)

[HIPAA]

3.4
accountability
property that ensures that the actions of an entity can be traced uniquely to the entity

[ISO 7498-2]

concept that individual persons or entities can be held responsible for specified actions

[NRC]

obligation to disclose periodically, in adequate detail and consistent form, to all directly and indirectly responsible or properly interested parties, the purposes, principles, procedures, relationships, results, incomes and expenditures involved in any activity, enterprise, or assignment so that they can be evaluated by the interested parties

[JCAHO]

3.5
actor
⟨with respect to an action⟩ an enterprise object (or entity) that participates in the action

[ISO/IEC 15414]

3.6
agent
enterprise object (or entity) that has been delegated (authority, a function, etc.) by and acts for another (in exercising the authority, performing the function, etc.)

[ISO/IEC 15414]

3.7
aggregate
aggregation
to combine standardized data and information

[JCAHO]

3.8
algorithm
algorithmic
series of steps for addressing a specific issue

[JCAHO]

3.9
application
identifiable computer running a software process

NOTE 1 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 In some jurisdictions, including software processes may be regulated medical devices.

3.10
architecture
set of principles on which the logical structure and interrelationships to an organization and business context are based

NOTE Software architecture is the result of software design activity.

3.11
archived (records)
archival (records)
⟨healthcare⟩ data saved for later reference or use, possibly off-line

[COACH]

3.12
assurance
grounds for confidence, surety, certitude

grounds for confidence that an entity meets its security objectives

[ISO/IEC 15408:1999]

development, documentation, testing, procedural and operational activities carried out to ensure a system's security services do in fact provide the claimed level of protection

[OMG 97]

3.13
asymmetric cryptographic algorithm
algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ

[ISO 10181-1]

3.14
audit control
mechanisms employed to record and examine system activity

[HIPAA]

3.15
audit trail
record of the resources which were accessed and/or used by whom

[ISO 7498-2]

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

[NRC]

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

[GCST]

3.16
authentication of health record entries
process used to verify that an entry is complete, accurate and final

[JCAHO]

3.17
authentication
providing assurance regarding the identity of a subject (author) or object (information)

[ASTM E1762]

3.18
authentication (data)
verification of the integrity of data that have been stored, transmitted or otherwise exposed to possible unauthorized modification

[GCST]

3.19
authentication (data source)
corroboration that the source of data received is as claimed

[ISO 7498-2]

3.20
authentication (user)
provision of assurance of the claimed identity of an entity

[ISO/IEC 10181-2]

3.21
authorize
authorization
granting of rights, which includes granting of access based on access rights

[ISO 7498-2]

prescription that a particular behaviour must not be prevented

[ISO/IEC 15414]

3.22
authorized user
user who may, in accordance with the Security Policy, perform an operation

[ISO/IEC 15408:1999]

3.23
availability
property of being accessible and useable upon demand by an authorized entity

[ISO 7498-2]

prevention of the unauthorized withholding of information or resources

[ITSEC]

3.24
biometric
biometrics
use of specific attributes that reflect unique personal characteristics, such as a fingerprint, an eye blood-vessel print, or a voice print, to validate the identity of entities

[ISO/IEC 2382-08]

3.25
business unit
discrete and accountable function or sub-function within an organization

NOTE For example, a business unit includes a department, service or speciality of a healthcare provider organization.

3.26
care
provision of accommodations, comfort and treatment to an individual subject of care (patient), also implying responsibility for safety

[JCAHO]

3.27
caregiver
cf. **healthcare professional** (3.76)

3.28
care plan
cf. **critical path** (3.47)

3.29
certificate
public key certificate
user certificate
public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it

[ISO 9594-8]

agreement that binds a user's name to a public key, signed by a trusted issuer

[NRC]

NOTE A framework for the use of public key certificates is defined in CCITT Standard X.509.

3.30
certificate policy
named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

[X.509]

3.31
certification
procedure by which a third party gives assurance that all or part of a data processing system conforms to security requirements

[ISO/IEC 2382-08]

administrative act of approving a system for use in a particular application

[NRC]

3.32
certification authority
CA
certificate issuer
authority trusted by one or more relying parties to create and assign certificates

[ISO 9594-8]

NOTE Optionally the certification authority may create the relying parties' keys.

3.33
ciphertext
data produced through the use of encipherment; the semantic content of the resulting content is not available

[ISO 7498-2]

3.34
classification level
security level of information

[NSC]

3.35
clearance level
permission granted to an individual to access information at or below a particular security level

[ISO/IEC 2382-08]

3.36
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

[CEN ENV 1613:1995]

data/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

[ASTM E1769, CPRI]

3.37
code set
any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes

[HIPAA]

3.38
coding scheme
collection of rules that maps the elements of one set on to the elements of a second set

[ISO/IEC 7826]

3.39
complete health record
final, assembled and authenticated, health record for an individual

(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

[JCAHO]

3.40
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

[ISO 7498-2]

condition in which information is shared or released in a controlled manner

[NRC]

prevention of the unauthorized disclosure of information

[ITSEC]

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

[JCAHO]

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

[OTA]

3.41
consent
voluntary agreement with what is being done or proposed (express or implied)

[CIHI]

communication process between the caregiver and the (subject of care), and which may refer to consent for treatment, special procedures, release of information and advance directives [which give instructions regarding the (subject of care's) wishes in special medical situations]

[CPRI]

3.42
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

[JCAHO]

3.43
constituency
class of persons served in common

NOTE A group of individuals and/or organizations with explicit common interests and who may elect or otherwise designate agents or delegates to represent such interests.

3.44
credentials (for identity)
data that are transferred to establish the claimed identity of an entity

[ISO/IEC 2382-08]

3.45
credentials (for healthcare practice)
documented evidence of (a healthcare professional's) licensure, education, training, experience, or other qualifications

[JCAHO]

3.46
criteria
expected level(s) of achievement, or specifications against which performance can be assessed

[JCAHO]

3.47
critical path(s)
care plan(s)
clinical pathway(s)
plan, based on data gathered during (subject of care) assessment, that identifies the care needs, lists the strategy for providing services to meet those needs, documents treatment goals and objectives, outlines the criteria for terminating specified interventions, and documents the (subject of care's) progress in meeting specified goals and objectives

[JCAHO]

3.48
cryptography
discipline, which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

[ISO 7498-2]

art of keeping data secret, primarily through the use of mathematical or logical functions that transform intelligible data into seemingly unintelligible data and back again

[NRC]

3.49
cryptographic algorithm
cipher
method for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

[ISO 7498-2]

3.50
data attribute, element or item
single unit of data that in a certain context is considered indivisible

[CEN ENV 13606-4]

3.51
data reliability
stability, repeatability, or precision of the data

[JCAHO]

3.52
data transmission
data transmittal
sending of data or information from one location to another location

[JCAHO]

exchange of data between person and program, or program and program, when the sender and receiver are remote from each other

[CPRI]

3.53
data validity
verification of correctness (reflecting the true situation)

[JCAHO]

3.54
decision support
(typically) electronic system designed to aid healthcare professionals make clinical decisions

3.55
decipherment
decryption
process of obtaining, from a ciphertext, the original corresponding data

[ISO/IEC 2382-8]

process of decoding a message so that its meaning becomes obvious

[OTA]

3.56
de-identified data
data resulting from personally identifiable information after the process of removing or altering one or more attributes so that the (direct or indirect) identification of the relevant person without knowledge of the initial information is either impossible or requires an unreasonable amount of time and manpower

[MEDSEC]

3.57
delegate
to give (authority, function, etc.) to another

[ISO/IEC 15414]

3.58
device
identifiable computer controlled apparatus or instrument that is the holder of a private encipherment key

NOTE This includes the class of regulated medical devices that meet the above definition. Device in this context is any device used in healthcare information systems including those without any direct role in treatment or diagnosis.

3.59
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 and integrity of the data unit and protect against forgery e.g. by the recipient

[ISO 7498-2]

electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified

[HIPAA]

NOTE 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.

3.60
disclosure (of health information)
release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information

[HIPAA]

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

[CPRI]

3.61
documentation
process of recording information in the (health) record

[JCAHO]

3.62
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)

[JCAHO]

3.63
electronic health record
EHR
electronic healthcare record
ECHR
health record concerning the subject of care in computer-readable form

[CEN ENV13606-1]

3.64
encipherment
encryption
cryptographic transformation of data (see cryptography) to produce ciphertext

[ISO 7498-2]

process of encoding a message so that its meaning is not obvious

[OTA]

3.65
episode of care
identifiable grouping of healthcare related activity characterized by the entity relationship between the subject of care and a healthcare provider, such a grouping determined by the healthcare provider

3.66
firewall
computer system providing an isolation layer between a private network security domain and a public untrusted network

[CIHI]

3.67
health information
any 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

[HIPAA]

3.68
health record
healthcare 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

[JCAHO]

3.69
health record entry
healthcare record entry
dataset, suitably attributed, which forms part of, or a whole, contribution to a health(care) record at one place and time

[CEN ENV 13606-2]

3.70
healthcare
care, services, or supplies related to the health of an individual

[HIPAA]

NOTE 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.

3.71
healthcare agent
medical devices (e.g. instruments, monitors) and software (e.g. applications, components) which: a) perform a role in the provision of healthcare services; and/or b) are accountable for actions related to, and/or ascribed in, the health record

[CEN ENV 12265, modified]

3.72
healthcare data
data which are input, stored, processed or output by the automated information system which support the clinical and business functions of a healthcare organization; these data may relate to person identifiable records or may be part of an administrative system where persons are not identified

[HL7]

3.73
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

[Directory of the European Standardization Requirements for Healthcare Informatics and Telematics v2.1, 1994]

3.74
healthcare organization
generic term used to describe many types of organizations that provide healthcare services

[JCAHO]

3.75
healthcare party
individuals, organizations or business units, including: a) subjects of care (patients, health plan members); b) those involved in the direct or indirect provision of healthcare services to an individual or to a population; and/or c) those accountable for actions related to, and/or ascribed in, the health record

[CEN ENV 1613:1995, modified]

3.76
healthcare professional
person that is authorized by a nationally recognized body to be qualified to perform certain health services

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

[CEN ENV 1613: 1995]

NOTE 1 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 Examples of health professionals are physicians, registered nurses and pharmacists.

3.77
healthcare provider
healthcare organization or healthcare professional responsible for the provision of healthcare to a subject of care or to a population

[CEN 13940:2000]

3.78
health plan
individual or group plan that provides, or pays the cost of, medical care

[HIPAA]

3.79
identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

[CEN ENV 13608-1]

3.80
indelible
indelibility
impossible to remove or erase, permanent

3.81
indicator (of performance)
measure used to determine over time, (an organization's) performance of functions, processes and outcomes

[JCAHO]

3.82
individually identifiable health information
any 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

[HIPAA]

3.83
information
interpreted set(s) of data that can assist in decision making

[JCAHO]

data to which meaning is assigned, according to context and assumed conventions

[NSC]

3.84
in-patient
subject of care who is admitted to a healthcare organization for an overnight stay, in order to receive healthcare

3.85
integrity (data)
property that data has not been altered or destroyed in an unauthorized manner

[ISO 7498-2]

accuracy, consistency and completeness of data

[JCAHO]

3.86
integrity (message)
proof that the message content has not altered, deliberately or accidentally in any way, during transmission

[ISO/IEC 7498-2]

3.87
interface
process that permits the flow of data from one system to another in a structured manner

3.88
interoperability
with regard to a specific task is said to exist between two applications when one application can accept data from the other and perform the task in an appropriate and satisfactory manner (as judged by the user of the receiving system) without the need for extra operator intervention

[CEN]

ability of software and hardware on multiple machines from multiple vendors to communicate; ability of a system to use the parts or equipment of another system

[HL7 Security SIG]

3.89
key
sequence of symbols that controls the operations of encipherment and decipherment

[ISO 7498-2]

3.90
key management
generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy

[ISO 7498-2]

3.91
longitudinal or lifetime personal health record
permanent, coordinated record of significant information, in chronological sequence; it 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

[ASTM E1384]

3.92
master file
dataset containing definitional entries in common across system, business units and, in some cases, organizational boundaries

NOTE 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.

3.93
master patient index
MPI
index within a given healthcare organization which serves as a directory to patients (subjects of care)

[CPRI]

3.94
measure
collect quantifiable data about a function or process

[JCAHO]

3.95
message
logically ordered dataset designed to communicate essential information between systems

3.96
need-to-know
legitimate requirement of a prospective recipient of data to know, to access, or to possess any sensitive information represented by these data

[ISO/IEC 2382-08]

users should have access only to the data he or she needs to perform a particular function

[HIPAA]

3.97
network
electronic data transmission facility which can comprise of just a point-to-point wire link between two devices, or a complex arrangement of transmission lines

3.98
non-repudiation (of origin, of submission, of receipt)
service that provides proof of the integrity and origin of data (both in an unforgeable relationship) which can be verified by any party

[ASTM]

proof (to a third party) that only the signer could have created a signature; basis of legal recognition of digital signatures

[ASTM E1762]

provision of evidence which will prevent a participant in an action from convincingly denying his/her responsibility for the action

[OMG]

3.99
object
identifiable, encapsulated entity that provides one or more services

[OMG]

3.100
organization
unique framework of authority within which a person or persons act, or are designated to act towards the same purpose

[ISO 6523:1984]

3.101
outcome
result of the performance (or non-performance) of a function or process(es)

[JCAHO]

3.102
out-patient
subject of care whose episode of care in a healthcare organization does not require an overnight (or less than 24 hour) stay in that same organization

3.103
party
object modelling a natural person or any other entity considered to have the same rights, powers and duties of a natural person

[ISO/IEC 15414]

3.104
patient
cf. **subject of care**

3.105
patient assessment
systematic collection and review of patient-specific data

[JCAHO]

3.106
patient reassessment
ongoing data collection that begins on initial assessment, comparing the most recent data with the data collected on the previous assessment

[JCAHO]

3.107
password
confidential authentication information composed of a string of characters

[ISO 7498-2]

sequence that an individual presents to a systems for purposes of authentication

[NRC]

3.108
payment guarantor
individual or organization responsible for the total or partial reimbursement or payment for the provision of healthcare services

[CEN ENV 13607]

3.109
performance
way in which an individual, group or organization carries out or accomplishes its important functions and processes

[JCAHO]

execution, accomplishment, fulfillment; operation or functioning, usually with regard to effectiveness

[Webster's New World Dictionary]

3.110
performance measure
measure, such as a standard or indicator, used to assess the performance of a function or process of any organization

quantification of processes and outcomes using one or more dimensions of performance, such as timeliness or availability

[JCAHO]

3.111
persistent
persistence
enduring

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

3.112
personal health information
any information that concerns a person's health, medical history, medical treatment or genetic characteristics in a form that enables the person to be identified

[MEDSEC]

3.113
personal information
any information relating to an identified or identifiable natural person

[EU Directive 95/46/EC, MEDSEC]

3.114
policies and procedures (for clinical care)
formal, approved description of how a governance, management of clinical care process is defined, organized and carried out

[JCAHO]

3.115
policy
set of rules related to a particular purpose; a rule can be expressed as an obligation, an authorization, a permission or a prohibition

[ISO/IEC 15414]

3.116
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

[JCAHO]

3.117
privacy
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

[ISO/IEC 2382-8]

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

[CPRI]

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

[HL7 Security SIG]

3.118
private key
key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity)

[ISO 10181-1]

NOTE This key may be used for encipherment, decipherment or signature generation.

3.119
process
collection of steps taking place in a prescribed manner and leading to the accomplishment of some result

[ISO/IEC 15414]

goal-directed, interrelated series of actions, events, mechanisms, or steps

[JCAHO]

3.120
protocol (care)
cf. **critical paths**

3.121
public key
key that is used with an asymmetric cryptographic algorithm and can be made publicly available

[ISO 10181-1]

NOTE This key may be used for encipherment, decipherment or signature verification.

3.122
public key certificate
X.509 public key certificates (PKCs) [X.509], binding an identity and a public key

[RFC2459, modified]

NOTE The identity may be used to support identity-based access control decisions after the client proves that it has access to the private key that corresponds to the public key contained in the PKC.

3.123
public key infrastructure
PKI
infrastructure used in the relation between a key holder and a relying party that allows a relying party to use a certificate relating to the key holder for at least one application using a public key dependent security service

NOTE PKI includes a Certification Authority, a certificate data structure, means for the relying party to obtain current information on the revocation status of the certificate, a certification policy and methods to validate the certification practice.

3.124
purpose (of a system)
practical advantage or intended effect of the system

[ISO/IEC 15414]

3.125
quality
totality of features and characteristics of a product, process or service that bear on its ability to satisfy its stated or intended needs

[CEN]

character, characteristic or property of anything that makes it good or bad, commendable or reprehensible; thus the degree of excellence that a thing possesses; totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implied needs; fitness for use

[JCAHO]

3.126
quality improvement
approach to the continuous study and improvement of the processes of providing healthcare services to meet the needs of patients and others

[JCAHO]

3.127
recovery
restoration of an information system back to an error-free and secure state from which normal operation can resume

[CEN]

3.128
registry
server capable of holding data for the systematic and continuous follow up of information objects maintained in accordance with specific rules

3.129
release of information
disclosure of documents containing (subject of care)-identifiable information to a third party requestor

[CPRI]

3.130
repudiation
denial by one of the entities involved in a communication of having participated in all or part of the communication

[ASTM E1762]

3.131
resource
enterprise object modelling an entity which is essential to some behaviour and which requires allocation or may become unavailable because it is in use or used up

[ISO/IEC 15414]

3.132
retention
maintenance and preservation of information in some form (e.g. paper, microfilm, or electronic storage) for a given period of time

[CPRI]

3.133
secondary record
record that is derived from the primary record and contains selected data elements

[ASTM E1384]

3.134
security
combination of availability, confidentiality, integrity and accountability

[CEN ENV 13608-1]

protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and 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

[NSC]

preservation of the confidentiality and integrity of data as well as ensuring the accountability and availability of data; combination of availability, confidentiality, integrity and accountability

[CEN ENV 12924, MEDSEC]

result of effective protection measures that safeguard data/information from undesired occurrences and exposure to accidental or intentional disclosure to unauthorized persons, accidental or malicious alteration, unauthorized copying, software deficiencies, operating mistakes, or sabotage

[IOM]

3.135
security (data)
protection of data from intentional or unintentional destruction, modification, or disclosure

[JCAHO]

3.136
security policy
plan or course of action adopted for providing computer security

[ISO/IEC 2382-8]

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

[DOD Orange Book]

framework within which an organization establishes needed levels of information security to achieve the desired confidentiality goals; statement of information values, protection responsibilities and organization commitment for a system; set of laws, rules and practices that regulate how an organization manages, protects and distributes sensitive information

[OTA]

3.137
standard
document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context

[ISO/IEC Guide 2: 1996]

NOTE Standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits.

3.138
step
task in a process

[ISO/IEC 15414]

3.139
subject of care
person or defined groups of persons receiving or registered as eligible to receive healthcare services or having received healthcare services

[CEN ENV 12443:1996]

NOTE For example, a patient, client, customer, or health plan member.

3.140
systematic
pursuing defined objective(s) in a planned, step-by-step manner

[JCAHO]

3.141
trust
confidence; a basis of reliance, faith, or hope; assured reliance on the character, strength, or truth of someone or something

[Merriam-Webster's Dictionary]

3.142
trusted system
system believed to enforce a given set of attributes to a stated degree of assurance (confidence)

[NRC]

system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information

[GCST]

4.143
use (of health information)
sharing, employment, application, utilization, examination, or analysis of such information

[HIPAA]

3.144
user
person or other entity authorized by a provider to use some or all of the services provided by the provider

[COACH]

human being using the system to issue requests to objects in order to get them to perform functions in the system on his/her behalf

[OMG]

4 Abbreviated terms

AHA	American Hospital Association
ANSI	American National Standards Institute
API	Application Program Interface
ASC X12	Accredited Standards Committee X12, an ANSI Accredited SDO
ASTM E31	American Society for Testing Materials, Committee E31 on Healthcare Informatics
DICOM	Digital Imaging and Communications in Medicine; standard developed by NEMA
CCITT	Consultative Committee on International Telephony and Telegraphy
CEN	Comité Européen de Normalisation, European Committee for Normalization
CIHI	Canadian Institute for Health Information
COACH	Canadian Organisation for the Advancement of Computers in Health (now Canadian Health Informatics Association)
CPRI	Computer-Based Patient Record Institute
DOD	U.S. Department of Defense
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport (also referred to as UN/EDIFACT)
EHR, EHCR	electronic health record, electronic healthcare record
ENV	CEN European Pre-Standard
GCST	US DOD Glossary of Computer Security Terms
HCFA	US DHHS Healthcare Financing Administration
HIPAA	Health Insurance Portability and Accountability Act of 1996, US Public Law 104-191
HISB	ANSI Healthcare Informatics Standards Board
HL7	Health Level Seven, an ANSI Accredited SDO
HMO	Health Management Organization
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IOM	Institute of Medicine, a body of the US National Institutes of Health

ISO	International Organization for Standardization
ISO TC215	ISO Technical Committee 215 on Healthcare Informatics
ITSEC	Information Technology Security Evaluation Criteria
JCAHO	Joint Commission for Accreditation of Healthcare Organizations
KC	Key Characteristic(s), the primary topic of this ISO Technical Report
MEDSEC	Healthcare Security and Privacy in the Information Society, project sponsored by the European Commission
MIB	IEEE Committee P1073, Medical Information Bus
NCQA	National Council for Quality Assurance (US)
NCVHS	U.S. DHHS National Council for Vital and Health Statistics
NEHRT	National Electronic Health Records Taskforce (Australia)
NEMA	National Electrical Manufacturers Association
NHS	National Health Service (UK)
NIST	National Institute for Standards and Technology (US)
NMB	ISO National Member Body
NRC	National Research Council (US)
NSC	National Security Council (US)
ODP	Open Distributed Processing
OLAP	On-Line Analytical Processing
OLTP	On-Line Transaction Processing
OMG	Object Management Group
OTA	Office of Technology Assessment (US)
PKC	Public Key Certificate
PKI	Public Key Infrastructure
RM-ODP	Reference Model for Open Distributed Processing
SDO	Standards Developing Organization
SIG	Special Interest Group
TR	ISO Technical Report
USHIK	U.S. Health Information KnowledgeBase, a data registry maintained by the U.S. DHHS (HCFA) and DOD
UN	United Nations
WEDI	Work Group for Electronic Data Interchange
WG2	ISO TC215, Working Group 2 on Messaging and Communications

5 Trust Constituency

The Trust Constituency consists of individuals, organizations and business units. The Trust Constituency relies substantially on ISO/TC 215 and its work products to protect and engage their rights and obligations with regard to health information interchange.

Table 1 identifies parties to the Trust Constituency.

Trust Constituency: for health record content, including individually identifiable information Constituent	Individual	Organization	Business unit	Subject of record	Accountable source, Author of record content	Accountable verifier of record content	Accountable scribe of record content	Accountable user of record content	Accountable record steward	Accountable provider of health services as documented in record
Subject of care, Health plan member	X			Yes	Yes	AA [b]	NA [a]	AA	No	No
Next of kin, Emergency contact	X			Yes	No	No	No	No	No	No
Healthcare professional, Caregiver	X			Yes	Yes	Yes	Yes	Yes	Yes	Yes
Care assistant	X			Yes	Yes	Yes	Yes	Yes	Yes	Yes
Transcriptionist	X			Yes	No	AA	Yes	AA	Yes	No
Department, Service, Speciality			X	Yes	NA	NA	NA	Yes	Yes	Yes
Healthcare provider	X	X		Yes	NA	NA	NA	Yes	Yes	Yes
Integrated delivery network (IDN)		X		Yes	NA	NA	NA	Yes	Yes	Yes
Payment guarantor, Health plan, HMO	X	X		AA	No	No	No	Yes	Yes	No
Value added network, Claims clearinghouse		X		No	No	No	No	Yes	Yes	No
Employer	X	X		AA	No	No	No	Yes	AA	No
Public health agency		X		No	No	No	No	Yes	AA	No
Regulatory agency		X		No	No	No	No	Yes	AA	No
Accreditation agency		X		No	No	No	No	Yes	AA	No
Research	X	X		No	No	No	No	Yes	AA	No
Professional education	X	X		No	No	No	No	Yes	AA	No
Others										

[a] Not applicable.
[b] As applicable.

Table 1 — The Trust Constituency (for health records and record interchange)

6 Principles and objectives

An essential foundation to the ISO/TC 215/WG 2 work program is a set of principles and objectives to enable trusted health information interchange.

Principles and objectives for the ISO/TC 215/WG 2 work programme:	Ensure trust in the veracity and protection of health records to all constituent parties **(Ensured Trust)**.
Design and/or adopt standards for healthcare messaging and communication which:	Recognize, ensure and protect the incumbent interests of all constituent parties **(Trust Constituency)**.
	Recognize and ensure fundamental **Health record rights**.
	Recognize and ensure fundamental **Health record obligations**.
	Ensure full representation of the **Health record and its composition**.
	Ensure full representation of **Healthcare parties and their accountable actions**.
	Ensure full representation of **Healthcare agents and their accountable actions**.
	Ensure full representation of healthcare parties and agents, their actions and corresponding **Scope of accountability (Unit of accountability)**.
	Ensure and enable the full set of services for **Authentication**: user, data source/origin, data verification, data interchange.
	Ensure **Auditability** of accountable parties and agents and their accountable actions.
	Ensure **Chain of trust** tracking in the course of information flow from point of origin (e.g. point of service/care) to point of use.
	Ensures faithfulness, permanence, persistence and indelibility of the health record and its content.
	Ensure robust methods **of Data definition,** including formalization and harmonization with recognized **Data registries**.
	Ensure vital aspects of **Data integrity,** including accuracy, context, consistency, comparability, continuity, completeness and relevance.
	Ensure vital aspects of **Completeness,** including completeness of the health delivery process, of the health record, of individual subject of care health records.

Table 2 — Principles and objectives (to ensure trusted health information interchange)

6.1 Ensured Trust

Constituent parties — individuals, organizations and business units — have a trust stake with regard to the veracity of the health record, including its origin, amendment, stewardship and use. With particular reference to:

a) Privacy and confidentiality;

b) Protection of individually identifiable information;

c) Protection during the course of interchange — “in transit”.

6.2 Trust Constituency

There are a multitude of constituent parties to the health record and its content, each with definitive rights and obligations (see clause 5):

a) As subjects of the health record, e.g.:

   1) Individual subjects of care, health plan members;

   2) Individual healthcare professionals, caregivers;

   3) Individual originators of record content: authors, scribes and verifiers;

   4) Organizations, including: providers, health plans;

   5) Business units, including: departments, services, specialities;

   6) Others, including: next of kin, emergency contacts, payment guarantors.

b) As parties participating in the provision, performance and completion of healthcare services and whose related actions are ascribed in the health record, e.g.:

   1) Individual healthcare professionals, caregivers;

   2) Organizations;

   3) Business units.

c) As parties participating in the origin, amendment, stewardship and use of the health record whose related actions are ascribed therein, e.g.:

   1) Individual healthcare professionals, caregivers;

   2) Individual authors, scribes and verifiers;

   3) Organizations;

   4) Business units.

Specific rights and obligations of constituent parties, in terms of the health record and its content, are designated variously by local legislation, regulations, standards of practice and custom, and are outside the scope of this Technical Report.

6.3 Health record rights

Health record rights include authentic information, which is complete, accurate and can be accessed by the record subject. Other crucial record rights include:

a) Confidentiality and privacy protections, particularly with regard to access to, use and disclosure of:

   1) Individually identifiable information;

2) Information subject to protection:

— by statute, regulation, standard of practice or custom; and/or

— by virtue of explicit disclosure grants and agreements;

3) Information made available by such grants and agreements:

— for purpose(s) intended;

— by those parties so authorized;

— for the period (of time) designated; and

— based on the principle of “need to know”.

b) Complete and accurate portrayal of health status and interventions;

c) Complete and accurate portrayal of the provision, performance and completion of health services;

d) Detailed audit logs tracking record creation, amendment, access, use and disclosure.

Specific health record rights are designated variously by local legislation, regulation, standards of practice and custom, and are outside the scope of this Technical Report.

6.4 Health record obligations

Health record obligations include accountability for:

a) Record content origination and amendment, as ascribed to authors, scribes and/or verifiers;

b) Provision, performance and completion of health services, as documented in the record and as ascribed to healthcare professionals, caregivers;

c) Accuracy, completeness of record content;

d) Access to, and use of, record content;

e) Duplication of record content;

f) Disclosure, transmission and receipt of record content;

g) Translation of record content (e.g. mapping to alternate coding and classification schemes).

Specific health record obligations are designated variously by local legislation, regulations, standards of practice and custom, and are outside the scope of this Technical Report.

6.5 Health record composition

In its fullest manifestation, the health record (of the subject of care) comprises:

a) A longitudinal chronology of health status and interventions;

b) A chronicle of health service events corresponding to the provision, performance and completion of healthcare services;

c) A collection of discrete record instances (e.g. documents), often corresponding in a 1:1 relationship with health service events.

6.6 Healthcare parties and their accountable actions

Healthcare parties are those individuals, organizations and business units accountable for actions related to, and/or ascribed in, the health record, including:

a) Origination or amendment of record content: as authors, scribes, verifiers;

b) Provision, performance and/or completion of healthcare services, specifically health service events;

c) Access to, and use of, record content;

d) Duplication of record content;

e) Disclosure, transmission and/or receipt of record content;

f) Translation of record content.

In many but not all cases, individuals as healthcare parties, act as agents/employees and/or on behalf of organizations and business units.

6.7 Healthcare agents and their accountable actions

Healthcare agents include medical devices (e.g. instruments, monitors) and software (e.g. applications, components) accountable for actions related to, and/or ascribed in, the health record, including:

a) Origination of record content (typically pre-verification);

b) Duplication of record content;

c) Transmission and/or receipt of record content;

d) Translation of record content.

Healthcare agents typically act within the domain, on behalf (or delegation) of and under the immediate control, of healthcare parties (as described above).

6.8 Scope of accountability, Unit of accountability

Accountable actions of healthcare parties, healthcare agents engage a corresponding scope of accountability. Such scope includes (the domain of) health record content ascribed to:

a) Healthcare parties in terms of their specific actions in the provision, performance and/or completion of health services;

b) Healthcare parties and agents in terms of their specific actions in the origination, amendment, stewardship and use of the record.

The scope of accountability can be reduced to a discrete unit of accountability, comprising a set of attributes (data elements):

c) Describing the performance, provision and/or completion of a discrete health service event;

d) Comprising a discrete record instance.

6.9 Authentication

Authentication is fundamental to the trusted interchange of healthcare information. It enables a recipient to reliably verify the parties to the origination, validation, transmittal and receipt of health records, in whole or in part. Specific authentication functions are crucial, these include:

a) User authentication: evidence of individual identity;

b) Data source/origin authentication: evidence of authorship, origination, amendment;

c) Data validation authentication: evidence of data verification, e.g.:

   1) of data originated by another party;

   2) of automated device input;

d) Data interchange authentication: evidence of data transmittal, receipt.

Additional aspects of authentication include:

e) Non-repudiation (e.g. of authorship);

f) Digital signature;

g) Public/private key infrastructure;

h) Encrypted encapsulation: binding record content to an authenticated source.

6.10 Auditability

Intrinsic to full accountability is the establishment of robust audit trails and audit review tools, sufficient to comprehensively track healthcare parties and agents and their accountable actions.

6.11 Chain of trust

As end-to-end information flows imply, there is an intrinsic need to track the chain of trust (i.e., chain of custody), including health record stewardship and as health records transit points of interchange, points of translation and points of convergence.

6.12 Faithfulness, permanence, persistence and indelibility

Another prerequisite is the need to ensure health records are faithfully maintained in a permanent, indelible, unaltered form, from point of origination to point of use. This includes:

a) Preservation of original content and context;

b) Revision by (additive) amendment only;

c) Preservation of discrete data states: for the original and each amendment;

d) Ability to reconstruct health records for any given historical date/time.

6.13 Data definition, Data registry

Concise data definition is the foundation to data integrity, including definitions of attributes (i.e. data elements) and data groups (e.g. minimum, core and reference datasets). Data registries, such as the U.S. Health Information

Knowledge base (USHIK), are a basic method to ensure the formalization and harmonization of attribute/data group definitions across SDOs, accreditation and governance bodies, and others.

6.14 Data integrity

Data integrity includes definitions of and measures for accuracy, context, consistency, comparability, continuity, completeness and relevance. Data reliability is integral to data integrity and includes stability, repeatability and precision. Data integrity is based on data definition, as described above, but also relies substantially on robust methods for information flow from the point of origination to the point of use.

6.15 Completeness and continuity

This requirement serves to ensure completeness and continuity:

a) In the process of healthcare delivery, including the completeness of discrete events, encounters and episodes;

b) In health records, including correlative documentation of the health delivery process;

c) In health records, pertaining to individual subjects of care, even though record subsets may be sourced independently at different times, by different locations, by different healthcare providers.

7 Key characteristics (KC)

7.1 Identifiable information

7.1.1 Interchange of identifiable individual or organization information

This messaging/communication KC covers the interchange of health records or information which may be identifiable to specific healthcare parties (i.e. individuals, organizations, business units), and/or which may include their distinguishing traits.

Examples where information identifiable to an individual healthcare party may be interchanged:

— Information interchange between multiple front-end clinical applications to manage the real-time health delivery process and work flow;

— Information interchange from clinical front-end applications to back-end repository;

— Information interchange to third parties (e.g. payers for claims, public health agencies for immunization, communicable disease registries).

7.1.2 Identifiable parties

Identifiable parties (may) include:

a) As subjects of the health record, e.g.:

1) Individual subjects of care;

2) Individual healthcare professionals, caregivers;

3) Individual originators of record content: authors, scribes and verifiers;

4) Organizations, including: providers, health plans;

5) Business units, including: departments, services, specialities;

6) Others, including: next of kin, emergency contacts, payment guarantors.

b) As parties participating in the provision, performance and completion of healthcare services and whose related actions are ascribed in the health record, e.g.:

1) Individual practitioners/caregivers;

2) Organizations;

3) Business units.

c) As parties participating in the origin, amendment, stewardship and use of the health record and whose related actions are ascribed therein, e.g.:

1) Individual healthcare professionals, caregivers;

2) Individual authors, scribes and verifiers;

3) Organizations;

4) Business units.

7.2 Architectural basis

7.2.1 General

This messaging/communication KC is based on a formalized architecture.

EXAMPLE Architectural template for interchange of information among and between multiple clinical, administrative and operational applications in a healthcare provider enterprise or integrated delivery network.

7.2.2 Architectural constructs

Architectural constructs (may) include the following details:

a) Data definition:

1) Health record and its subsets;

2) Data groups: datasets, templates;

3) Attributes: data elements;

4) Identifiers;

5) Business objects, relationships;

6) Versioning.

b) Information model:

1) Business classes (objects);

2) Subject areas;

3) Subject classes (i.e., stateful classes);

4) Attributes, identifiers;

5) Relationships between classes, attributes;

6) Vocabulary, coding, classification;

7) Audit;

8) Versioning.

c) Business operations (process) model:

1) Actors (including accountable parties and agents);

2) Actions (including accountable actions);

3) States, state/transitions;

4) Work flow;

5) Audit.

d) Information flow model:

1) End-to-end:

— Point of origination (point of service/care) to point of use;

— Front-end to back-end to third party;

2) Stewardship, chain of trust;

3) Audit.

e) Application interoperability model:

For applications or software components:

1) Application role(s);

2) Application interactions: as sender, as receiver;

— Trigger events;

— Unsolicited updates;

— Query/response;

— Receipt acknowledgment;

3) Inter-application relationships:

— Point-to-point interaction model: paired sender, receiver roles;

— Inter-dependencies;

4) Application binding:

— API: tightly coupled, passed parameters, delegated control;

— Message: loosely coupled (e.g. ASTM, DICOM, EDI/EDIFACT, HL7, MIB);

— Mediated interchange (e.g. via interface engines, hubs);

i) En-route queuing, store and forward;

ii) En-route translation, transformation: of data groups, of attributes;

iii) Phase I acknowledgement: mediator to transmitter;

iv) Phase II acknowledgement: receiver to mediator;

v) End-to-end acknowledgement: receiver to transmitter;

vi) Phase I threaded message sequence: transmitter to mediator;

vii) Phase II threaded message sequence: mediator to receiver;

viii) End-to-end threaded message sequence: transmitter to receiver;

— Security, access control;

— Audit;

— Clock synchrony;

— Data synchrony;

— Transactions, multi-phase commits (to synchronous data stores);

— Data definition;

— Master files;

— Master registries;

5) Versioning.

f) Security, Access control model:

1) Access control;

2) Classifications: for information, functions;

3) Clearances: for users, roles;

4) Security policy domains;

5) Authentication: user, data source, data verification, data transmittal/receipt;

6) Non-repudiation;

7) Digital signature;

8) Audit.

g) Accountability model (integral to the Security, Access control model):

   1) Accountable parties/agents;

   2) Accountable actions.

h) Vocabulary model:

   1) Vocabulary domains;

   2) Coding, classification schemes, including version.

7.3 Master files

7.3.1 General

EXAMPLE Synchronous master file updates via interchange among all applications serving a health provider enterprise.

This messaging/communication KC specifies the interchange of master file definition information.

For such interchange, messages (may) include:

a) Synchronize, across 2-n master files:

   1) At initial application binding;

   2) Dynamic, in real-time;

   3) Individual definition instance;

   4) 2-n definition instances;

   5) All definition instances.

b) Find/match definition instance, using matching identifier(s) and/or trait(s);

c) Update definition instance, including identifier(s) and/or trait(s) and including actions to: originate, amend/translate;

d) Verify definition instance;

e) Activate/deactivate definition instance;

f) List audit trail for definition instance;

g) Update audit trail for definition instance, including actions to: access, originate, amend/translate, verify, transmit, receive;

h) Enable master file transaction, multi-phase commit: bid, open/lock, update, close/unlock;

i) Archive definition record(s).

7.3.2 Master file: Data definition

Data definitions (may) include:

a) Health records and subsets thereof:

   1) Personal health record: for individual subject of care, health plan member;

2) Population health record;

3) Business (operations) record: for organizations, business units;

4) Personal service record: for individual healthcare professional, caregiver.

b) Data groups (datasets, templates):

1) Naming, identifier(s);

2) Precise usage;

3) Aggregated attributes (contained therein);

4) At the data group level, measures and rules for: accuracy, context, consistency, comparability, continuity, completeness, relevance.

c) Attributes (data elements):

1) Naming, identifier(s);

2) Precise usage;

3) Data type, format;

4) Classification, coding scheme, including version;

5) Range;

6) At the attribute level, measures and rules for: contextual data (attribute) relationships, accuracy, consistency, comparability, continuity, completeness, relevance.

d) Business classes (objects):

1) Naming, identifier(s);

2) Precise usage;

3) Relationships with other business objects;

4) Aggregated attributes (contained therein);

5) At the class level, measures and rules for: accuracy, context, consistency, comparability, continuity, completeness, relevance.

7.3.3 Master file: Context set/Template definition

Context set definitions (may) include:

a) Accountability context;

b) Data integrity context;

c) Clinical context;

d) Operational context.

7.3.4 Master file: Function definition

Function definitions (may) include:

a) Information access, management and processing functions.

7.3.5 Master file: Security classification definition

Security classification definitions (may) include:

a) Classification level of information, for aggregations or units of information: e.g.

   1) Health records and subsets thereof;

   2) Data groups (datasets);

   3) Attributes (data elements).

b) Access permissions for information: e.g. access/use, originate, amend/translate, verify, duplicate, disclose, transmit, receive;

c) Classification of functions: e.g. for information access, management and processing functions, for firewalls installed;

d) Access permissions for functions: e.g. access, process.

7.3.6 Master file: Security clearance definition

Security clearance definitions (may) include:

a) Clearances for accountable healthcare parties: individuals, organizations, business units;

b) Clearances for accountable healthcare roles.

7.3.7 Master file: Security policy domain definition

Security policy domain definitions (may) include:

a) Security policy domains: organization-wide, by business unit (e.g. department, service, speciality).

7.3.8 Master file: Orders, Order set definition

Order, order set definitions (may) include:

a) Orderable health services: e.g. therapeutic, diagnostic, care services;

b) Orderable medications;

c) Orderable healthcare resources: staff, locations, equipment, supplies, time.

7.3.9 Master file: Health services, Service event definition

Services, service event definitions (may) include:

a) Health services: e.g. therapeutic, diagnostic, care;

b) Related medications, if any;

c) Related resource parameters: e.g. staff, locations, equipment, supplies;

d) Related schedule/time parameters: e.g. frequency, duration.

7.3.10 Master file: Protocol definition

Protocol definitions (may) include:

a) Protocols: e.g. care plans, critical paths;

b) Related health services;

c) Related conditions and interdependencies;

d) Events, tasks, sequence and staging.

7.3.11 Master file: Decision support rule definition

Decision support definitions (may) include:

a) Rules, conditions, resulting actions.

7.3.12 Master file: Facility and location definition

Facility and location definitions (may) include:

a) Organization: facilities;

b) Business units: departments, services, specialities;

c) Nursing units, rooms, beds.

7.3.13 Master file: Resource definition

Resource definitions (may) include:

a) Staff;

b) Facilities/locations;

c) Equipment;

d) Supplies;

e) Time/duration.

7.3.14 Master file: Charge and cost definition

Charge and cost definitions (may) include:

a) Health services;

b) Staff;

c) Facilities/locations;

d) Equipment;

e) Supplies;

f) Time/duration.

7.4 Master registries

7.4.1 Accountable healthcare parties

This messaging/communication KC specifies the interchange of registry information sufficient to enable a master registry to be constructed of accountable healthcare parties, including individuals, organizations and business units. Each accountable healthcare party may be known by one or more identifiers, may be assigned one or more healthcare roles and may be afforded access privileges under one or more security clearances (see 6.6).

The information content of this registry may include one or more of: personal identifiers, demographics, contact information, licenses/credentials, role(s), security clearance(s), access details (e.g. passwords, biometrics), activation status, affiliations (e.g. practice group, organization), privileges, business unit (department, service, speciality), etc.

EXAMPLE A master registry of healthcare professionals, caregivers and system users for a healthcare provider enterprise, for an integrated delivery network.

For the interchange of registry information, messages (may) include:

a) Synchronize, across 2-n registries:

   1) At initial application binding;

   2) Dynamic, in real-time;

   3) Individual party instance;

   4) 2-n party instances;

   5) All party instances in registry.

b) Find/match party instance, using identifier(s) and/or trait(s);

c) Update party instance, its identifier(s) and/or trait(s), including actions to: originate, amend/translate;

d) Verify party instance;

e) Activate/deactivate party instance;

f) Enable/disable party's security clearances: for access to information, to functions;

g) Merge/unmerge party instances;

h) List audit trail for party instance;

i) Update audit trail for party instance, including actions to: access, originate, amend/translate, verify, activate/deactivate, enable/disable security clearances, merge/unmerge, transmit, receive;

j) Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock;

k) Archive party instance.

7.4.2 Accountable healthcare roles

This messaging/communication KC specifies the interchange of registry information sufficient to enable a master registry of accountable healthcare roles, particularly with regard to:

— Provision, performance and/or completion of health services;

— Origination, amendment, stewardship and use of the health record.

Each role may be afforded access privileges under one or more security clearances.

EXAMPLES Attending physician, resident, registered nurse, respiratory therapist, pharmacist, clinical consultant, physician's assistant, transcriptionist, clerk, as well as specialists such as radiologists, pathologists, cardiologists.

For the interchange of registry information, messages (may) include:

a) Synchronize, across 2-n registries:

   1) At initial application binding;

   2) Dynamic, in real-time;

   3) Individual role instance;

   4) 2-n role instances;

   5) All role instances in registry.

b) Find/match role instance, using identifier(s) and/or trait(s);

c) Update role instance, its identifier(s) and/or trait(s), including actions to: originate, amend/translate;

d) Verify role instance;

e) Activate/deactivate role instance;

f) Enable/disable role's security clearances, for access to information, to functions;

g) Merge/unmerge role instances;

h) List audit trail for role instance;

i) Update audit trail for role instance, including actions to: access, originate, amend/translate, verify, activate/deactivate, enable/disable security clearances, merge/unmerge, transmit, receive;

j) Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock;

k) Archive role instance.

7.4.3 Accountable healthcare agents

This messaging/communication KC specifies the interchange of registry information sufficient to enable a master registry of accountable healthcare agents, including devices and application software (see 6.7).

EXAMPLES Devices: bedside monitors, ventilators, IV pumps, lab instruments, dispensing devices; software: patient registration/admission/discharge/transfer, bedside, laboratory, radiology, pharmacy, order entry, scheduling, workflow, medication administration, nursing, ancillaries.

For the interchange of registry information, messages (may) include:

a) Synchronize, across 2-n registries:

   1) At initial application binding;

   2) Dynamic, in real-time;

   3) Individual agent instance;

   4) 2-n agent instances;

   5) All agent instances in registry.

b) Find/match agent instance, using identifier(s) and/or trait(s);

c) Update agent instance, its identifier(s) and/or trait(s), including actions to: originate, amend/translate;

d) Verify agent instance;

e) Activate/deactivate agent instance;

f) List audit trail for agent instance;

g) Update audit trail for party instance, including actions to: access, originate, amend/translate, verify, activate/deactivate, transmit, receive;

h) Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock;

i) Archive agent instance.

7.4.4 Subjects of care (persons)

This messaging/communication KC specifies the interchange of registry information sufficient to enable and maintain a master registry of individual subjects of care (e.g. patients and health plan members).

EXAMPLES Registry of persons served by a healthcare provider enterprise, by a health plan, by an integrated delivery network; registry of persons receiving clinical services.

For the interchange of registry information, messages (may) include:

a) Synchronize, across 2-n registries:

   1) At initial application binding;

   2) Dynamic, in real-time;

   3) Individual person instance;

   4) 2-n person instances;

   5) All person instances in registry.

b) Find/match person instance, using identifier(s) and/or trait(s);

c) Update person instance, its identifier(s) and/or trait(s), including actions to: originate, amend/translate;

d) Verify person instance;

e) Merge/unmerge person instances;

f) Link/unlink person instance to encounter;

g) Link/unlink person instance to another person instance;

h) Enable/disable role's security clearances, for access to information, to functions;

i) List audit trail for person instance;

j) Update audit trail for person instance, including actions to: access, originate, amend/translate, verify, merge/unmerge, link/unlink encounters, link/unlink persons, enable/disable security clearances, transmit, receive;

k) Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock;

l) Archive person instance.

7.4.5 Local identifier assignment

This messaging/communication KC specifies the interchange of information sufficient to enable and track local identifier assignment.

EXAMPLES

— Subject of care/health plan member ID: e.g. medical record number;
— Healthcare professional ID: e.g. license, certificate number;
— Employee, user ID;
— Encounter, episode ID;
— Financial account ID;
— Business unit ID: e.g. department, service, speciality ID;
— Location ID;
— Health service ID: e.g. procedure ID;
— Equipment, property tag/ID;
— Local product ID.

7.5 Electronic records

7.5.1 Personal health record

This messaging/communication KC specifies the interchange of the personal health record and its subsets. The personal health record chronicles the health status and interventions for an individual subject of care. The information content of the personal health record (may) include: personal identifiers and demographics, environmental, social and financial/coverage information, allergies, clinical interventions, problems/episodes of care, visits/encounters, personal schedule, consents, disclosures, health services received, medication profile, audit, etc.

EXAMPLE Subject of care-centred electronic health record system serving a health provider enterprise or an integrated delivery network.

For the interchange of personal health record(s), messages (may) include:

a) Synchronize, across 2-n health record systems:

1) At initial application binding;

2) Dynamic, in real-time;

3) Personal health record;

4) 2-n personal health records;

5) All personal health records.

b) Update audit trails for personal health record interchange: access, amend/translate, transmit, receive;

c) Enable interchange based on security classifications, security clearances and data definitions;

d) Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock;

e) Archive personal health record;

f) Enable multi-media record: text, audio, video, image/graphic, waveform, binary.

7.5.2 Population health record

This messaging/communication KC specifies the interchange of information related to a population health record. A population health record may comprise the aggregation or summaries of many personal records and may not contain information identifiable or selectable to an individual subject of care.

EXAMPLE Extractions, aggregations and summaries for performance, quality assurance and outcome reporting, utilization, public health, epidemiology, clinical research, etc.

For the interchange of population health record(s), messages (may) include:

a) Synchronize, population health record, across 2-n health record systems:

1) At initial application binding;

2) Dynamic, in real-time.

b) Update audit trails for population health record interchange: access, amend/translate, transmit, receive;

c) Enable interchange based on security classifications, security clearances and data definitions;

d) Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock;

e) Archive population health record;

f) Enable multi-media record: text, audio, video, image/graphic, waveform, binary.

7.5.3 Business (operations) record

This messaging/communication KC specifies the interchange of information related to a business (operations) record. A business record defines and chronicles the operations of an organization or business unit, including services performed/provided, historical and current status. It may or may not contain information identifiable or selectable to an individual subject of care.

EXAMPLE The business (operations) record and its subsets: policies, procedures, standards of practice/care, guidelines, schedules, allocations, deployments, assigned responsibility, work flow, performance, compliance, utilization, productivity, quality assurance, costs, services rendered, outcomes, audit, legal, etc.

For the interchange of business record(s), messages (may) include:

a) Synchronize business record, across 2-n record systems:

   1) At initial application binding;

   2) Dynamic, in real-time.

b) Update audit trails for business record interchange: access, amend/translate, transmit, receive;

c) Enable interchange based on security classifications, security clearances and data definitions;

d) Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock;

e) Archive business records;

f) Enable multi-media record: text, audio, video, image/graphic, waveform, binary.

7.5.4 Personal healthcare professional service record

This messaging/communication KC specifies the interchange of information related to a personal healthcare professional service record. A personal service record chronicles assignments and services performed/provided by an individual healthcare professional/caregiver, including current status.

EXAMPLE The personal service record and its subsets: assigned responsibility, personal schedule, services rendered, audit, etc.

For the interchange of personal service record(s), messages (may) include:

a) Synchronize personal service record, across 2-n record systems:

   1) At initial application binding;

   2) Dynamic, in real-time.

b) Update audit trails for personal service record interchange: access, amend/translate, transmit, receive;

c) Enable interchange based on security classifications, security clearances and data definitions;

d) Enable transaction, multi-phase commit: bid, open/lock, update, close/unlock;

e) Archive personal service record(s);

f) Enable multi-media record: text, audio, video, image/graphic, waveform, binary.

7.6 Record chronology, continuity, completeness

7.6.1 Chronological order of events

This messaging/communications KC specifies the interchange of information sufficient to describe a chronology of events and corresponding records, for:

a) Personal health record;

b) Population health record;

c) Business (operations) record;

d) Personal healthcare professional service record.

EXAMPLES Longitudinal subject of care health record; business operations log; time-based population study extracts for clinical or outcomes research; history of subject of care contacts for a healthcare professional (e.g. to ascertain exposure to infectious disease).

7.6.2 Event timeline

This messaging/communications KC specifies the interchange of information sufficient to describe an event timeline.

a) Prospective (future): events scheduled, not yet underway;

b) Concurrent (now): events in progress, not yet completed;

c) Retrospective (historical): events completed (or cancelled), in terminus state.

EXAMPLES Health history for an individual subject of care; health service events in progress, not yet complete; forthcoming health service events including wellness checks and scheduled preventative interventions.

7.6.3 Historical snapshot

This messaging/communications KC specifies the interchange of information sufficient to recreate the state of the health delivery process and the health record (or subset thereof) for an historical date/time either for a point in time or for a period of time.

EXAMPLE Snapshot of the personal health record at the moment of a critical clinical decision, viewed after the fact.

7.6.4 Continuity, completeness

This messaging/communications KC specifies the interchange of information sufficient to ensure the continuity and completeness of the health record.

EXAMPLE Encounter-oriented health record completion summary: What's incomplete? Who's responsible? Is the encounter complete, ready to close? Can it be final billed?

Relevant continuity/completeness functions (may) include:

a) Completeness metrics: for the health record and its subsets, for data groups (i.e. datasets), attributes (i.e. data elements);

b) Gap analysis.

7.7 Authentication, non-repudiation services

7.7.1 User authentication

This messaging/communications KC specifies the interchange of information sufficient to ensure user authentication, including evidence of identity of accountable healthcare parties and their accountable actions.

EXAMPLE Trusted identity of users, healthcare professionals, caregivers.

7.7.2 Data source authentication

This messaging/communications KC specifies the interchange of information sufficient to ensure data source authentication, including evidence of identity of accountable healthcare parties/healthcare agents and their accountable actions of authorship, or to originate or amend health record content.

EXAMPLE Trusted identity of health record content authors, scribes.

7.7.3 Verification authentication

This messaging/communications KC specifies the interchange of information sufficient to ensure verification authentication, including evidence of identity of accountable healthcare parties and their accountable actions to verify health record content.

EXAMPLE Trusted identity of health record content verifiers (e.g. content authored by another, data input from an automated device).

7.7.4 Data interchange authentication

This messaging/communications KC specifies the interchange of information sufficient to ensure data interchange authentication, including evidence of identity of accountable healthcare parties and their accountable actions to disclose, transmit or receive health record content.

EXAMPLES Trusted identity of transmitters and receivers, firewall installation.

7.7.5 Non-repudiation services

This messaging/communication KC specifies the interchange of information sufficient to enable trusted non-repudiation services.

EXAMPLE Non-repudiation services for health record authorship, origination, amendment, verification, duplication, disclosure, transmission, receipt.

7.8 Digital signature, Public key infrastructure

7.8.1 Digital signature

This messaging/communications KC specifies the interchange of information sufficient to enable a robust digital signature methodology. A digital signature binds the identity of an accountable healthcare party and affirmation of their accountable action(s) to health record content and/or to the performance, provision and completion of clinical service events. This binding also establishes the scope of accountability.

EXAMPLES Trusted affirmation of authorship of health record content, trusted affirmation of responsibility for the performance or provision of healthcare services.

7.8.2 Public key infrastructure (PKI)

This messaging/communications KC specifies a digital signature based on trusted certification authorities and a public key infrastructure.

EXAMPLE Public/private keys, relying on asymmetric cryptographic algorithms.

7.9 Audit

7.9.1 Audit trails

This messaging/communications KC specifies the interchange of information sufficient to track the accountable actions of accountable healthcare parties.

EXAMPLE 1 Audit log showing the stream of events emanating from a laboratory service order: place order, verify order, draw specimen, accession specimen, analyse specimen, post preliminary results, verify and sign final results, post final results, post supplemental or corrected results.

EXAMPLE 2 Audit log showing the stream of events emanating from a radiology service order: place order, verify order, schedule examination room, schedule subject of care NPO, transport subject of care, check subject of care into department/ examination room, perform examination, check subject of care out, transport subject of care back to nursing unit, perform initial

review of examination results, dictate preliminary report, transcribe report, review and revise report, transcribe revisions, review and sign final report, post final report.

Audit trails (may) track:

a) Provision, performance and/or completion of healthcare services, and specifically health service events: as healthcare professionals and caregivers;

b) Access to, and use of, health record content;

c) Origination or amendment of health record content: as authors, scribes;

d) Verification of health record content;

e) Duplication of health record content;

f) Disclosure, transmission or receipt of health record content;

g) Translation of health record content;

h) Escrow agreement provided and sealed.

7.9.2 Audit review

This messaging/communications KC specifies the interchange of information sufficient to enable review of audit trail detail.

EXAMPLE Audit log showing users or healthcare professionals accessing the personal health record for subjects of care to which they are not assigned (e.g. fellow employees, celebrity cases).

7.10 Permanence, persistence, indelibility

This message/communications KC specifies interchange of information sufficient to ensure the permanence, persistence and indelibility of the health record.

EXAMPLE 1 Trusted persistence of health record content unaltered from its point of origin to its point of use.

EXAMPLE 2 Audit logs showing content at origination and with each successive amendment.

Relevant persistence functions (may) include:

a) Preservation of the health record and its subsets, data groups and attributes;

b) Indelibility of content as originated;

c) Formal amendment process, preserving previous content;

d) Data state preservation: initial and through each amendment (addition only).

7.11 On-Line Transaction Processing (OLTP)

EXAMPLE 1 Real-time, highly integrated electronic health record system encompassing a health provider organization and its business units, an integrated delivery network.

EXAMPLE 2 Highly interactive electronic health record system, supporting prospective, concurrent, retrospective views of the health delivery process and health record chronology.

EXAMPLE 3 Tightly coupled applications, components and devices.

EXAMPLE 4 Synchronous data stores.

7.11.1 Tightly coupled OLTP services

This messaging/communications KC specifies tightly coupled interchange services sufficient to support real-time, high performance On-Line Transaction Processing (OTLP).

7.11.2 Multi-phase commit

This messaging/communications KC specifies tightly coupled interchange services sufficient to support multi-phase commits across synchronous data stores: e.g. bid, open/lock, update, close/unlock.

7.12 On-Line Analytical Processing (OLAP)

EXAMPLE 1 OLAP data warehouse for retrospective aggregation, derivation, summary, reporting of business (operational) and clinical information.

EXAMPLE 2 Executive information systems.

This messaging/communications KC specifies the interchange of information sufficient to support On-Line Analytical Processing applications (e.g. a data warehouse).

7.13 Fault tolerance

EXAMPLE Fault tolerant architecture supporting continuous healthcare operations (i.e. $24 \times 7 \times 365$), for a healthcare provider organization, for an integrated delivery network.

7.13.1 Redundant communications architecture

This messaging/communications KC specifies a redundant communication architecture sufficient to support fault tolerant interchange.

7.13.2 Unavailability/Failure detection

This messaging/communications KC specifies a real-time failure detection architecture, sufficient to determine the non-operational (unavailable) status of communicant devices and applications.

7.13.3 Availability/Restart detection

This messaging/communications KC specifies a real-time detection architecture sufficient to determine the operational (available) status of communicant devices and applications, including those just restarted.

7.13.4 Downtime and slow response queuing

This messaging/communications KC specifies a message queuing scheme sufficient to buffer interchange in the case of downtime or slow response cycles between communicant applications and devices.

7.13.5 Recovery

This messaging/communications KC specifies a method of post-downtime restart and recovery, in the case where one or more applications and/or devices have been unavailable for a period.

7.14 Data synchrony

EXAMPLE Multiple applications or components with independent data stores requiring synchronization services, across a healthcare provider organization, across an integrated delivery network.

This messaging/communications KC specifies the interchange of information sufficient to ensure the logical synchronization of information and data stores across communicant applications, components and devices:

a) At the initial binding;

b) At restart;

c) Continuously in normal operation.

7.15 Time synchrony

EXAMPLE Multiple applications or components requiring time synchronization services, across a healthcare provider organization, across an integrated delivery network.

This messaging/communications KC specifies the interchange of information sufficient to maintain, within an agreed tolerance, time synchrony across communicant applications, components and devices:

a) At initial binding;

b) At restart;

c) At periodic intervals in normal operation.

7.16 Trusted end-to-end information flows

EXAMPLE 1 Assurance that health record content persists from its point of origin (point of service/care) to a specific point of use.

EXAMPLE 2 Assurance of origination when, where and by whom indicated.

EXAMPLE 3 Assurance of accountability and chain of trust.

EXAMPLE 4 Assurance of data integrity.

EXAMPLE 5 Assurance of essential clinical and operational context.

EXAMPLE 6 Assurance of firewall integrity.

7.16.1 General

This messaging/communications KC is based on an architecture sufficient to ensure trusted end-to-end information flows, from the point of origin (point of service/care) to the point of use. In the course of such flow, information (typically in the form of messages) may traverse:

a) One or more points of interchange: i.e. interfaces between applications/devices;

b) One or more points of translation: e.g. where content is translated from one coding/classification scheme to another;

c) One or more points of convergence: e.g. where aggregation, derivation or summarization may occur.

7.16.2 End-to-end record audit

This messaging/communications KC specifies the interchange of information sufficient to reliably audit its flow from the point of origin to the point of use, tracking accountable actions of accountable healthcare parties/agents.

EXAMPLE Audit log showing detailed record history: e.g. create record, verify and sign record, amend record, disclose/transmit record, translate record content, receive record, steward record, access/use record.

Major audits (may) include:

a) Provision, performance and/or completion a health service event (typically the real-world trigger event initializing the information flow);

b) Access to, and use of, the health record or information;

c) Origination or amendment of health record or information;

d) Verification of health record or information;

e) Duplication of health record or information;

f) Disclosure, transmission or receipt of health record or information;

g) Translation of health record or information;

h) Stewardship of health record or information (i.e. data at rest);

i) Firewall installation.

7.16.3 Chain of trust audit

This messaging/communications KC specifies the interchange of information sufficient to reliably track the health record or its subset from point of origination to point of use — effectively a chain of trust — including traversals of points of interchange and points of translation.

EXAMPLE Audit log with entries for each accountable healthcare agent in the chain of trust (i.e. along the end-to-end interchange continuum).

7.16.4 Context sets, templates

This messaging/communications KC specifies interchange of information sufficient to enable context sets (templates) from the point of origination to the point of use.

EXAMPLE 1 Context sets/templates which persist from the point of record origin (point of service/care) to the point of use.

EXAMPLE 2 Context sets/templates describing the essential context of a clinical service event.

Context sets, templates (may) include:

a) Accountability context, describing:

   1) Who, what, when, where, why, how.

b) Data integrity context, describing rules, measures and indicators for information/data:

   1) Accuracy;

   2) Context;

   3) Comparability, consistency;

   4) Continuity, completeness;

   5) Relevance.

c) Clinical context, describing:

   1) Rationale;

   2) Clinical parameters;

   3) Clinical context and conditions;

   4) Measures of continuity and completeness (e.g. of the clinical service event);

   5) Measures of compliance (e.g. with standards of care/practice);

   6) Performance measures;

   7) Quality indicators;

   8) Outcome indicators.

d) Operational context, describing:

   1) Allocation, deployment;

   2) Assigned responsibility;

   3) Resource utilization (e.g. for staff, time, facilities, equipment, supplies);

   4) Costs;

   5) Productivity.

7.17 Disclosure, Export

EXAMPLE 1 Assurance of controlled and authorized disclosure of personal health information, based on explicit permissions and need to know, to specified parties, for purposes/uses described.

EXAMPLE 2 Audit logs of disclosures of health records and information.

7.17.1 Disclosure consent (authorization), scope, purpose

This message/communications KC specifies interchange of information sufficient to track consents (authorizations) for disclosure.

Authorization functions (may) include:

a) Subject of care consent (authorization) for release of information;

b) Scope of information eligible for disclosure;

c) From whom;

d) To whom;

e) For what purpose;

f) For what duration.

7.17.2 Controlled disclosure tracking

This message/communications KC specifies interchange of information sufficient to track actual disclosure of sensitive or protected content.

Services (may) include:

a) Disclosure, transmittal audits;

b) Receipt audits.

7.17.3 Disclosure labelling

This message/communications KC specifies interchange of information sufficient to ensure labelling of disclosed content as sensitive or protected, as applicable.

7.17.4 De-identification, aliasing

This message/communications KC specifies interchange of information sufficient to ensure de-identification or aliasing of data exports, as applicable.

Related services (may) include de-identification or aliasing of:

a) Identifiers for individuals, organizations, business units;

b) Personal demographics and traits;

c) Sensitive/protected information related to:

   1) Individual subjects of care;

   2) Individual healthcare professionals, caregivers;

   3) Organizations, business units.

7.18 Prospective services

7.18.1 Subject of care schedule

This message/communications KC specifies interchange of information sufficient to enable a prospective health schedule for subjects of care.

EXAMPLE Subject of care-centred enterprise-wide schedule.

Schedule features (may) include:

a) Integrated schedule across multiple care disciplines, business units: departments, services, specialities;

b) Integrated schedule encompassing all venues and encounter types: in-patient, emergent, ambulatory, long-term care, home care;

c) Timeline based, including forthcoming clinical service events;

d) Wellness, preventative and follow-up events;

e) Initiated by healthcare professional orders, order sets;

f) Initiated by protocols: e.g. care plans, critical paths;

g) Medication profile, medication events.

7.18.2 Assigned responsibility

This message/communications KC specifies interchange of information sufficient to enable assigned responsibility for scheduled clinical service events, based on business and clinical practice rules.

EXAMPLE 1 Assurance of assigned responsibility for performance, provision and completion of clinical service events.

EXAMPLE 2 Assurance of assigned responsibility for completion of health record entries: as author, as scribe, as verifier.

Assignment features (may) include:

a) Assignments to specific individual healthcare professional;

b) Assignments to a healthcare group;

c) Assignments to a healthcare role.

7.18.3 Healthcare professional schedule

This message/communications KC specifies interchange of information sufficient to enable a prospective schedule for healthcare professionals, caregivers, groups and roles.

EXAMPLE Healthcare professional-centred enterprise-wide schedule and work list.

Schedule features (may) include:

a) Timeline based, including forthcoming events;

b) Assigned responsibility;

c) Business and clinical rules based.

7.18.4 Resource schedule

This message/communications KC specifies interchange of information sufficient to enable a prospective resource-based schedule.

EXAMPLE 1 Resource oriented enterprise-wide schedule.

EXAMPLE 2 Ambulatory appointment scheduling: e.g. for clinics, exam rooms, procedure rooms.

EXAMPLE 3 Surgery scheduling: in-patient or out-patient.

Schedule features (may) include:

a) Business and clinical rules based;

b) Resource factors:

   1) Facilities, locations;

   2) Staff resource factors;

   3) Time resource factors;

   4) Equipment resource factors;

   5) Supply resource factors.

c) Review options:

1) By individual subject of care;

2) By individual healthcare professional;

3) By healthcare group or role;

4) Across/by organization or business unit: department, service, speciality;

5) By resource: facility, location, equipment, time slot.

7.18.5 Projections

This message/communications KC specifies interchange of information sufficient to enable critical operational projections, on a prospective basis.

EXAMPLE 1 Cost projections.

EXAMPLE 2 Resource projections: facilities, locations, staff, equipment, supplies, time.

Projection features (may) include:

a) Optimized projections regarding resource allocations, deployments;

b) Optimized projections of cost;

c) Business and clinical rule based.

7.19 Work flow

7.19.1 General

This message/communications KC specifies interchange of information sufficient to enable and track operational work flow.

EXAMPLE Real-time, work flow engine integrated across a healthcare provider organization, an integrated delivery network.

Work flow features (may) include:

a) Real-time, interactive work flow management;

b) Shared work flow management:

1) Among associated healthcare professionals, groups;

2) Across and among disciplines, business units;

3) Across multiple venues and encounter types: in-patient, emergent, ambulatory, long-term care, home care.

c) Based on tight integration of prospective schedules: subject of care, healthcare professional, resource;

d) Allocation, deployment of critical resources: facilities, locations, staff, equipment, supplies, time, etc.;

e) Work flow services:

   1) Initiate, assign;

   2) Allocate, deploy (resources);

   3) Condition;

   4) Stage, sequence, route;

   5) Track, checkpoint, status;

   6) Complete.

f) Initiation:

   1) By orders, order sets;

   2) By protocols: e.g. care plans, critical paths.

g) Threading:

   1) Single-threaded work flow: tasks in sequence;

   2) Multi-threaded work flow: tasks in parallel.

h) Inter-dependencies: tightly coupled tasks;

i) Based on business and clinical practice rules.

7.19.2 Continuity, Completeness

This message/communications KC specifies interchange of information sufficient to ensure the continuity and completeness of work flow and the corresponding healthcare delivery process.

EXAMPLE Work flow, healthcare delivery process completion summary: What's incomplete? Where are the gaps? Who's responsible?

Continuity, completeness services (may) include:

a) Completeness metrics;

b) Continuity monitors, from initiation through completion;

c) Gap analysis.

7.20 Concurrent status, Records

7.20.1 Concurrent subject of care status

This message/communications KC specifies interchange of information sufficient to concurrently track subject of care health status and related healthcare delivery services.

EXAMPLES Real-time, subject of care-centred status tracking: e.g.

— Current health status;

— Current problems, symptoms, diagnoses;

— Personal schedule of forthcoming events;

— Events in progress, current status;
— Current problem-oriented episodes, active problem list, milestones, status;
— Current protocols (e.g. care plans, critical paths): status, milestones, variances;
— Current encounters, visits;
— Current facilities, locations of care;
— Current medications;
— Current diagnostics, results, status;
— Current therapeutic interventions, results, status;
— Currently assigned healthcare professionals, caregivers.

7.20.2 Concurrent healthcare professional status

This message/communications KC specifies interchange of information sufficient to concurrently track healthcare professional status and related healthcare delivery services.

EXAMPLE Real-time, healthcare professional-centred tracking of assigned responsibilities and incomplete work list.

7.21 Retrospective status, Records

7.21.1 Retrospective subject of care record

This message/communications KC specifies interchange of information sufficient to retrospectively track health status and healthcare delivery services.

EXAMPLE 1 Real-time, subject of care-centred history:

— Previous health status;
— Previous problems, symptoms, diagnoses;
— Events complete or cancelled, in terminus status;
— Previous problem-oriented episodes;
— Previous protocols (e.g. care plans, critical paths): milestones, variances;
— Previous encounters, visits;
— Previous facilities, locations of care;
— Previous medications;
— Previous diagnostics, results;
— Previous therapeutic interventions, results;
— Previously assigned healthcare professionals, caregivers.

EXAMPLE 2 Archived, archival health records.

7.22 Personal healthcare professional services

7.22.1 Personal healthcare professional portal

This message/communications KC specifies interchange of information sufficient to support a personalized healthcare professional portal.

EXAMPLE Personal portal to the electronic health record for a healthcare provider organization, for an integrated delivery network.

Personal healthcare professional portal features (may) include:

a) Assigned responsibilities, incomplete work list: personal and/or for affiliated healthcare group;

b) Action items (e.g. items requiring signature);

c) Notifications, prompts, alerts, reminders;

d) E-mail functions;

e) Significant, unreviewed events since last access (e.g. new critical results);

f) Based on personalized criteria.

7.22.2 Personalized functions

This message/communications KC specifies interchange of information sufficient to enable functions personalized to individual healthcare professionals, caregivers.

EXAMPLE Based a practitioner's own criteria, personal:

— Views of the health record and its subsets;

— Orders, order sets;

— Protocols;

— Decision support, decision agents.

7.23 Data integrity

This message/communications EC specifies interchange of information sufficient to ensure data integrity: accuracy, context, consistency, comparability, continuity, completeness, relevance.

EXAMPLES

— Assurance of uniform data definition;

— Assurance of uniform data context, comparability;

— Assurance of uniform vocabulary, coding and classification;

— Assurance of data integrity in the course of interchange from point of origin (point of service/care) to point of use.

Data integrity services (may) include:

a) Uniform data definition, at various levels of data granularity:

   1) Public data registry (e.g. USHIK);

   2) Health record and its subsets;

   3) Data groups (i.e. datasets);

   4) Attributes (i.e. data elements).

b) Measures and indicators for accuracy, context, consistency, comparability, continuity, completeness, relevance;

c) Systematic, uniform data capture;

d) Consistent, structured content;

e) Consistent vocabulary, coding and classification.

7.24 Protocols: Care plans, Critical paths

7.24.1 Protocol basis

This message/communications EC specifies interchange of information sufficient to enable protocol customization.

EXAMPLES

— Standard clinical protocols from recognized authorities: e.g. professional societies;

— Protocols defined for particular diagnoses, disease states;

— Protocols defined for organizations, business units: e.g. department, services, specialities;

— Protocols defined for individual healthcare professionals or groups.

7.24.2 Protocol management

This message/communications EC specifies interchange of information sufficient to enable real-time protocol management.

EXAMPLE Real-time highly integrated protocol management engine for subjects of care served by a healthcare provider organization, by an integrated delivery network.

Protocol management features (may) include:

a) Immediate, interactive review of protocol status: by individual subject of care (patient, health plan member);

b) Real-time protocol variance monitor;

c) Protocol override, variance authorization.

7.25 Problem lists

This message/communications KC specifies interchange of information sufficient to enable real-time problem list management.

EXAMPLE Real-time highly-integrated problem list manager for subjects of care served by a healthcare provider organization, by an integrated delivery network.

Problem list features (may) include:

a) Immediate, interactive review of current problem list: by individual subject of care (patient, health plan member);

b) Current problem definition, status, milestones;

c) Current problem in terms of corresponding protocols: care plans, critical paths;

d) Current problem in terms of assigned responsibilities;

e) Review of previous problems: problem, milestones, final resolution/status.

7.26 Decision support

This message/communications EC specifies interchange of information sufficient to enable decision support.

EXAMPLES

— Real-time decision agents interactive at the point of service/care;

— Background decision agents scanning for particular conditions and initiating relevant notifications.

Decision support features (may) include:

a) Real-time, concurrent decision support:

   1) At the point of service/care;

   2) At the point of completion of clinical service events: e.g. results, interventions, observations.

b) Retrospective decision support: e.g. data warehousing;

c) Based on:

   1) Business and clinical practice rules;

   2) Practice guidelines, standards of care;

   3) Protocols;

   4) Performance measures;

   5) Quality indicators;

   6) Outcome indicators;

   7) Cost parameters.

d) Detection of:

   1) Duplicate/redundant clinical services;

   2) Conflicts and interactions.

e) Condition predicated actions, to:

   1) Initiate notifications, prompts, alerts, reminders;

   2) Initiate orders, order sets;

   3) Initiate, modify protocols;

   4) Initiate, cancel, hold clinical service events.

f) Link decision support based actions into health record.

7.27 Surveillance, Metrics and Analysis

7.27.1 Measures and indicators

This message/communications KC specifies interchange of information sufficient to enable definitions, rules, measures and indicators with regard to key aspects of clinical and operational performance and quality.

EXAMPLE 1 Definitions, rules, measures and indicators for clinical aspects, including:

— Continuity, completeness: of the healthcare or operations record, of work flow and the health delivery process;

— Compliance: e.g. with standards of practice/care;

— Performance, effectiveness;

— Quality, quality improvement;

— Outcomes;

— Protocols, variances.

EXAMPLE 2 Definitions, rules and measures and indicators for operational aspects, including:

— Allocation, deployment;

— Assigned responsibility;

— Resource utilization: facilities, locations, staff, equipment, supplies, time;

— Costs;

— Productivity, workload.

7.27.2 Epidemiological surveillance

This message/communications KC specifies interchange of information sufficient to enable epidemiological surveillance.

EXAMPLES

— Epidemiological surveillance of provider facilities and physical locations, nursing units, patient rooms, surgery suites, exam rooms, corridors, elevators, etc;

— Epidemiological surveillance of relevant clinical parameters: lab results, medication orders, etc.

7.28 Communications infrastructure

This message/communications KC specifies interchange of information sufficient to ensure timely and reliable information conveyance.

EXAMPLE Optimized communications infrastructure for a healthcare provider organization and its business units or an integrated delivery network.

Communication services (may) include:

a) Real-time, immediate information conveyance: e.g. point of origination (point of service/care) to point of use;

b) Notifications, prompts, alerts, reminders;

c) E-mail functions;

d) Telephone replacement functions;

e) Paper replacement functions;

f) Affirmative acknowledgement of receipt: by individual healthcare professionals, caregivers.

7.29 Multiple person linkage

This message/communications KC specifies interchange of information sufficient to enable the logical linkage of multiple persons.

EXAMPLES

— Next of kin, family members;

— Mother/child;

— Multiple birth, including sequence;

— Donor/recipient;

— Payment guarantor, guarantee;

— Insured, subscriber, health plan member;

— Emergency contact(s).

7.30 Healthcare professional — Subject of care linkage

This message/communications KC specifies interchange of information sufficient to enable the logical linkage of subjects of care and healthcare professionals.

EXAMPLE Assured linkage of healthcare professionals with assigned responsibility for a given subject of care.

7.31 Localization, Local authority

This message/communications KC specifies interchange of information sufficient to enable localization.

EXAMPLES

— Local business and clinical practice rules;

— Local language, vocabulary, code sets;

— Local adaptation per business unit, organization or integrated delivery network.

Localization requirements (may) include:

a) Security, access control:

   1) Security policies, policy domains;

   2) Classifications: for functions, information;

   3) Clearances: for users, roles.

b) Identifiers;

c) Accountable healthcare parties, agents;

d) Accountable healthcare roles;

e) Accountable healthcare groups;

f) Data definitions: health record and its subsets, data groups, attributes;

g) Context sets, templates;

h) Business and clinical practice rules;

i) Practice guidelines, standards of care;

j) Orders, order sets;

k) Services, service events;

l) Work flow;

m) Protocols: care plans, critical paths;

n) Decision support rules, conditions, actions;

o) Facilities, locations;

p) Charges, costs;

q) Surveillance, metrics and analysis: rules, measures and indicators, etc.

7.32 User environments

This message/communications KC specifies interchange of information sufficient to support multiple discrete user environments.

EXAMPLES

— Production;

— Test, development;

— Education, training.

7.33 Version management

This message/communications KC specifies interchange of information sufficient to enable version management and rollover to new revisions.

EXAMPLE Versioned constructs include:

— Application, component or device software;

— Vocabulary: code sets, classification schemes;

— Master definition files;

— API standards;

— Message, EDI standards: e.g. ASTM, CEN, DICOM, EDI/EDIFACT, HL7, MIB;

— Network, communications standards.

7.34 Inter-application interoperability

7.34.1.1 General

EXAMPLES

— API based applications and components conjoined in a tightly coupled manner to support a healthcare provider organization or integrated delivery network;

— Interconnected applications and components joined in a loosely coupled message-based interface scheme.

7.34.2 Application roles

This message/communications KC specifies interchange of information sufficient to enable specific application/component roles, as explicitly described.

7.34.3 Application interactions

This message/communications KC specifies interchange of information sufficient to support typical application/component interaction paradigms.

Relevant paradigms (may) include:

a) Trigger events;

b) Unsolicited updates;

c) Query/response;

d) Receipt acknowledgement.

7.34.4 Inter-application relationships

This message/communications KC specifies interchange of information sufficient to enable typical inter-application/component relationships.

Relevant relationships (may) include:

a) Point-to-point interaction model: paired sender/receiver;

b) Inter-dependencies.

7.34.5 Inter-application services

This message/communications KC specifies interchange of information sufficient to enable typical inter-application/component services.

Services (may) include:

a) API: tightly coupled, passed parameters, delegated control;

b) Message: loosely coupled (e.g. ASTM, DICOM, EDI/EDIFACT, HL7, MIB);

c) Mediated message interchange (e.g. via interface engines, hubs):

   1) En-route queuing, store and forward;

   2) En-route translation, transformation: of data groups, of attributes;

   3) Phase I acknowledgement: mediator to transmitter;

   4) Phase II acknowledgement: receiver to mediator;

   5) End-to-end acknowledgement: receiver to transmitter;

   6) Phase I threaded message sequence: transmitter to mediator;

   7) Phase II threaded message sequence: mediator to receiver;

   8) End-to-end threaded message sequence: transmitter to receiver.

d) Security, access control;

e) Audit;

f) Clock synchrony;

g) Data synchrony;

h) Transactions, multi-phase commits (to synchronous data stores);

i) Data definition;

j) Master files;

k) Master registries.

7.35 Change scale (Scalability)

This message/communications KC specifies interchange of information sufficient to enable broad extensibility and change of scale of health record systems and the environments they support.

EXAMPLES

— Change scale from small to medium to large healthcare provider organization;

— Change scale to a large integrated delivery network;

— Change scale from few to many subjects of care, health plan members;

— Change scale from few to many healthcare professionals;

— Change scale from few to many interconnected applications, components and devices;

— Change scale from encounter based health record to lifetime subject of care health record;

— Change scale from few to many transactions per unit time;

— Change scale without appreciable performance barriers.

7.36 Validation

This message/communications KC has evidenced substantial, broad-based validation in the environments to which it is targeted and in terms of the purposes for which it is intended.

EXAMPLES

— Validation in number of vendor products supporting production implementations;

— Validation in number of discrete sites implemented;

— Validation in diversity and scale of implementations.

8 Principles and objectives enabled by key characteristics

PRINCIPLES AND OBJECTIVES	ENABLED BY… KEY CHARACTERISTICS
6.1 Ensured Trust	7.1 Identifiable information 7.2 Architectural basis 7.3 Master files 7.4 Master registries 7.5 Electronic records 7.6 Record chronology, continuity, completeness 7.7 Authentication, non-repudiation services 7.8 Digital signature, Public key infrastructure 7.9 Audit 7.10 Permanence, persistence, indelibility 7.14 Data synchrony 7.15 Time synchrony 7.16 Trusted end-to-end information flows 7.17 Disclosure, Export 7.20 Concurrent status, Records 7.21 Retrospective status, Records 7.23 Data integrity 7.28 Communications infrastructure 7.34 Inter-application interoperability 7.36 Validation
6.2 Trust Constituency	7.1 Identifiable information 7.2 Architectural basis 7.3 Master files 7.4 Master registries 7.5 Electronic records 7.6 Record chronology, continuity, completeness 7.7 Authentication, non-repudiation services 7.8 Digital signature, Public key infrastructure 7.9 Audit 7.10 Permanence, persistence, indelibility 7.16 Trusted end-to-end information flows 7.17 Disclosure, Export 7.20 Concurrent status, Records 7.21 Retrospective status, Records 7.23 Data integrity 7.28 Communications infrastructure 7.30 Healthcare professional — Subject of care linkage 7.31 Localization, Local authority 7.36 Validation

PRINCIPLES AND OBJECTIVES	ENABLED BY… KEY CHARACTERISTICS
6.3 Health record rights	7.1 Identifiable information 7.2 Architectural basis 7.3 Master files 7.4 Master registries 7.5 Electronic records 7.6 Record chronology, continuity, completeness 7.7 Authentication, non-repudiation services 7.8 Digital signature, Public key infrastructure 7.9 Audit 7.10 Permanence, persistence, indelibility 7.16 Trusted end-to-end information flows 7.17 Disclosure, Export 7.20 Concurrent status, Records 7.21 Retrospective status, Records 7.23 Data integrity 7.28 Communications infrastructure 7.29 Multiple person linkage 7.30 Healthcare professional — Subject of care linkage 7.36 Validation
6.4 Health record obligations	7.1 Identifiable information 7.2 Architectural basis 7.3 Master files 7.4 Master registries 7.5 Electronic records 7.6 Record chronology, continuity, completeness 7.7 Authentication, non-repudiation services 7.8 Digital signature, Public key infrastructure 7.9 Audit 7.10 Permanence, persistence, indelibility 7.16 Trusted end-to-end information flows 7.17 Disclosure, Export 7.20 Concurrent status, Records 7.21 Retrospective status, Records 7.23 Data integrity 7.28 Communications infrastructure 7.30 Healthcare professional — Subject of care linkage 7.36 Validation

PRINCIPLES AND OBJECTIVES	ENABLED BY… KEY CHARACTERISTICS
6.5 Health record composition	7.1 Identifiable information 7.2 Architectural basis 7.3 Master files 7.4 Master registries 7.5 Electronic records 7.6 Record chronology, continuity, completeness 7.7 Authentication, non-repudiation services 7.8 Digital signature, Public key infrastructure 7.9 Audit 7.10 Permanence, persistence, indelibility 7.18 Prospective services 7.19 Work flow 7.20 Concurrent status, Records 7.21 Retrospective status, Records 7.22 Personal healthcare professional services 7.23 Data integrity 7.24 Protocols: Care plans, Critical paths 7.25 Problem lists 7.26 Decision support 7.27 Surveillance, Metrics and Analysis 7.29 Multiple person linkage 7.30 Healthcare professional — Subject of care linkage 7.31 Localization, Local authority 7.36 Validation
6.6 Healthcare parties and their accountable actions	7.1 Identifiable information 7.4 Master registries 7.5 Electronic records 7.6 Record chronology, continuity, completeness 7.7 Authentication, non-repudiation services 7.8 Digital signature, Public key infrastructure 7.9 Audit 7.10 Permanence, persistence, indelibility 7.16 Trusted end-to-end information flows 7.17 Disclosure, Export 7.18 Prospective services 7.19 Work flow 7.20 Concurrent status, Records 7.21 Retrospective status, Records 7.22 Personal healthcare professional services 7.23 Data integrity 7.24 Protocols: Care plans, Critical paths 7.26 Decision support 7.28 Communications infrastructure 7.30 Healthcare professional — Subject of care linkage 7.36 Validation

PRINCIPLES AND OBJECTIVES	ENABLED BY… KEY CHARACTERISTICS
6.7 Healthcare agents and their accountable actions	7.1 Identifiable information 7.4 Master registries 7.7 Authentication, non-repudiation services 7.8 Digital signature, Public key infrastructure 7.9 Audit 7.10 Permanence, persistence, indelibility 7.16 Trusted end-to-end information flows 7.17 Disclosure, Export 7.18 Prospective services 7.19 Work flow 7.23 Data integrity 7.28 Communications infrastructure 7.34 Inter-application interoperability 7.36 Validation
6.8 Scope of accountability, Unit of accountability	7.1 Identifiable information 7.5 Electronic records 7.6 Record chronology, continuity, completeness 7.7 Authentication, non-repudiation services 7.8 Digital signature, Public key infrastructure 7.9 Audit 7.10 Permanence, persistence, indelibility 7.16 Trusted end-to-end information flows 7.17 Disclosure, Export 7.23 Data integrity 7.36 Validation
6.9 Authentication	7.1 Identifiable information 7.4 Master registries 7.5 Electronic records 7.7 Authentication, non-repudiation services 7.8 Digital signature, Public key infrastructure 7.9 Audit 7.10 Permanence, persistence, indelibility 7.23 Data integrity 7.31 Localization, Local authority 7.34 Inter-application interoperability 7.35 Change scale (Scalability) 7.36 Validation

PRINCIPLES AND OBJECTIVES	ENABLED BY… KEY CHARACTERISTICS
6.10 Auditability	7.1 Identifiable information 7.2 Architectural basis 7.4 Master registries 7.5 Electronic records 7.6 Record chronology, continuity, completeness 7.7 Authentication, non-repudiation services 7.8 Digital signature, Public key infrastructure 7.9 Audit 7.10 Permanence, persistence, indelibility 7.15 Time synchrony 7.16 Trusted end-to-end information flows 7.17 Disclosure, Export 7.19 Work flow 7.20 Concurrent status, Records 7.21 Retrospective status, Records 7.23 Data integrity 7.28 Communications infrastructure 7.31 Localization, Local authority 7.34 Inter-application interoperability 7.35 Change scale (Scalability) 7.36 Validation
6.11 Chain of trust	7.1 Identifiable information 7.2 Architectural basis 7.5 Electronic records 7.6 Record chronology, continuity, completeness 7.7 Authentication, non-repudiation services 7.8 Digital signature, Public key infrastructure 7.9 Audit 7.10 Permanence, persistence, indelibility 7.16 Trusted end-to-end information flows 7.17 Disclosure, Export 7.20 Concurrent status, Records 7.21 Retrospective status, Records 7.23 Data integrity 7.28 Communications infrastructure 7.31 Localization, Local authority 7.34 Inter-application interoperability 7.36 Validation

PRINCIPLES AND OBJECTIVES	ENABLED BY… KEY CHARACTERISTICS
6.12 Faithfulness, permanence, persistence and indelibility	7.2 Architectural basis 7.5 Electronic records 7.6 Record chronology, continuity, completeness 7.9 Audit 7.10 Permanence, persistence, indelibility 7.14 Data synchrony 7.16 Trusted end-to-end information flows 7.23 Data integrity 7.31 Localization, Local authority 7.34 Inter-application interoperability 7.35 Change scale (Scalability) 7.36 Validation
6.13 Data definition, Data registry	7.1 Identifiable information 7.2 Architectural basis 7.3 Master files 7.5 Electronic records 7.11 On-Line Transaction Processing (OLTP) 7.12 On-Line Analytical Processing (OLAP) 7.16 Trusted end-to-end information flows 7.23 Data integrity 7.27 Surveillance, Metrics and Analysis 7.31 Localization, Local authority 7.34 Inter-application interoperability 7.35 Change scale (Scalability) 7.36 Validation
6.14 Data integrity	7.2 Architectural basis 7.3 Master files 7.5 Electronic records 7.6 Record chronology, continuity, completeness 7.7 Authentication, non-repudiation services 7.8 Digital signature, Public key infrastructure 7.9 Audit 7.10 Permanence, persistence, indelibility 7.14 Data synchrony 7.16 Trusted end-to-end information flows 7.23 Data integrity 7.27 Surveillance, Metrics and Analysis 7.31 Localization, Local authority 7.36 Validation

Annex A

Exercise to validate the key characteristics set out in this technical report

A.1 General

Members of the ISO/TC 215/WG 2 Medical Devices Sub-Group based at the Heinrich-Heine-Universität Hospital, Düsseldorf, Germany devised a flow chart of activity (Figure A.1) to illustrate the different levels of communication to be found between a Hospital Information System (Level 2) i.e. a patient Health Record Server and a Departmental Computer System (Level 1) in an Intensive Care Unit (ICU), device-orientated environment. Different levels of communication are evident in many other sectors of the healthcare domain, for example, general medical practitioner clinic/hospital specialist clinic; community pharmacy/hospital pharmacy; community nursing, hospital nursing.

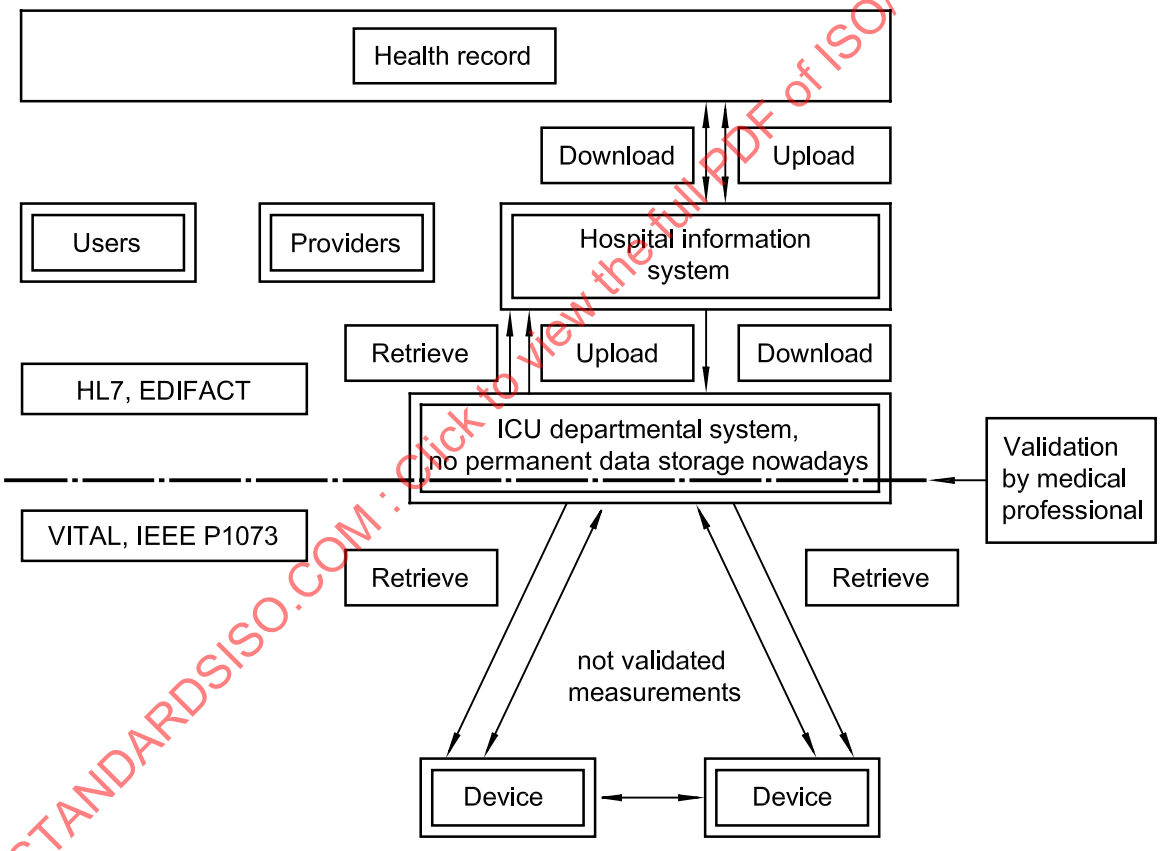

Figure A.1 — Flow chart of communication flows in a hospital environment

The Düsseldorf team subsequently used the key characteristics listed in the Technical Report to validate the recommendations in the Report. The resulting Tables demonstrate that the key characteristics listed are a valuable check list of the components required to develop complete message packages.

Table A.1 addresses the applicability of Principles and objectives, Section 6, to the “Level 1” and “Level 2” domains.

Table A.2 addresses the applicability of the Key characteristics, Section 7, to the “Level 1” and “Level 2” domains.

Table A.1 — Applicability of principles and objectives to HIS and departmental systems

	Principles and objectives	Dept. system to HIS	Device to dept. system
6.1	**Ensured Trust**	Yes	Yes
a)	Privacy and confidentiality;	Yes	Yes
b)	Protection of individually identifiable information;	Yes	Yes
c)	Protection during the course of interchange — “in transit”.	Yes	Yes
6.2	**Trust Constituency**	Yes	NA
a)	Subjects of the health record;	Yes	NA
b)	Parties participating in the provision, performance and completion of healthcare services and whose related actions are ascribed in the health record;	Yes	NA
c)	Parties participating in the origination, amendment, stewardship and use of the health record and whose related actions are ascribed therein.	Yes	NA
6.3	**Health record rights**	Yes	NA
a)	Confidentiality and privacy protections, particularly with regard to access to, use and disclosure of:		
1)	Individually identifiable information;	Yes	NA
2)	Information subject to protection:	Yes	NA
—	by statute, regulation, standard of practice or custom; and/or	Yes	NA
—	by virtue of explicit disclosure grants and agreements;	Yes	NA
3)	Information made available by such grants and agreements:	Yes	NA
—	for purpose(s) intended;	Yes	NA
—	by those parties so authorized;	Yes	NA
—	for the period (of time) designated; and	Yes	NA
—	based on the principle of “need to know”.	Yes	NA
b)	Complete and accurate portrayal of health status and interventions;	Yes	NA
c)	Complete and accurate portrayal of the provision, performance and completion of health services;	Yes	NA
d)	Detailed audit logs tracking record creation, amendment, access, use and disclosure.	Yes	NA
6.4	**Health record obligations**		
a)	Record content origination and amendment, as ascribed to authors, scribes and/or verifiers;	Yes	NA
b)	Provision, performance and completion of health services, as documented in the health record and as ascribed to healthcare professionals, caregivers;	Yes	NA
c)	Accuracy, completeness of record content;	Yes	NA
d)	Access to, and use of, record content;	Yes	NA
e)	Duplication of record content;	Yes?	NA
f)	Disclosure, transmission and receipt of record content;	Yes	NA
g)	Translation of record content (e.g. mapping to alternate coding and classification schemes).	Yes	NA
6.5	**Health record composition**		
a)	A longitudinal chronology of subject of care health status and interventions;	(Yes)	NA
b)	A chronicle of health service events corresponding to the provision, performance and completion of healthcare services;	(Yes)	NA
c)	A collection of discrete record instances (documents), often corresponding in a 1:1 relationship with health service events.	(Yes)	NA

Table A.1 *(continued)*

	Principles and objectives	Dept. system to HIS	Device to dept. system
6.6	**Healthcare parties and their accountable actions**		
a)	Origination or amendment of record content: as authors, scribes, verifiers;	Yes	NA
b)	Provision, performance and/or completion of healthcare services, specifically health service events;	Yes	NA
c)	Access to, and use of record content;	Yes	NA
d)	Duplication of record content;	?	NA
e)	Disclosure, transmission and/or receipt of record content;	Yes	NA
f)	Translation of record content.	?	NA
6.7	**Healthcare agents and their accountable actions**		
a)	Origination of record content (typically pre-verification);	Yes	Yes
b)	Duplication of record content;	?	NA
c)	Transmission and/or receipt of record content;	Yes	Yes
d)	Translation of record content.	?	NA
6.8	**Scope of accountability, Unit of accountability**		
a)	Healthcare parties in terms of their specific actions in the provision, performance and/or completion of health services;	NA	NA
b)	Healthcare parties and agents in terms of their specific actions in the origination, amendment, stewardship and use of the record;	NA	NA
c)	Describing the performance, provision and/or completion of a discrete health service event;	Yes?	NA
d)	Comprising a discrete record instance.	Yes?	NA
6.9	**Authentication**		
a)	User authentication: evidence of individual identity;	Yes	?
b)	Data source/origin authentication: evidence of authorship, origination, amendment;	Yes	Yes
c)	Data validation authentication: evidence of data verification, e.g.:		
1)	Of data originated by another party;	No?	NA
2)	Of automated device input.	Yes	NA
d)	Data interchange authentication: evidence of transmission, receipt;		?
e)	Non-repudiation (e.g. of authorship);	?	NA
f)	Digital signature;	Yes	NA
g)	Public/private key infrastructure;	?	NA
h)	Encrypted encapsulation: binding record content to an authenticated source.	?	?
6.10	**Auditability**	Yes	NA
6.11	**Chain of trust**	Yes	NA
6.12	**Faithfulness, permanence, persistence and indelibility**		NA
a)	Preservation of original content and context;	Yes	NA
b)	Revision by (additive) amendment only;	Yes	NA
c)	Preservation of discrete data states: for the original and each amendment;	Yes	NA
d)	Ability to reconstruct health records for any given historical date/time.	Yes	NA
6.13	**Data definition, Data registry**	Yes	?
6.14	**Data integrity**	Yes	Yes
6.15	**Completeness and continuity**		

Table A.2 — Applicability of key characteristics to HIS and departmental systems

	Key characteristics	Dept. system to HIS	Device to dept. system
7.1	**Identifiable information**		
7.1.1	**Interchange of identifiable individual or organization information**		
7.1.2	**Identifiable parties**		
a)	As subjects of the health record:		
1)	Individual subjects of care;	Yes	Yes?
2)	Individual healthcare professionals, caregivers;	Yes	NA
3)	Individual originators of record content: authors, scribes and verifiers;	Yes	NA
4)	Organizations, including: providers, health plans;	NA?	NA
5)	Business units, including: departments, services, specialities;	Yes	NA
6)	Others, including: next of kin, emergency contacts, guarantors.	Yes?	NA
b)	As parties participating in the provision, performance and completion of healthcare services and whose related actions are ascribed in the health record:		
1)	Individual practitioners/caregivers;	Yes	NA
2)	Organizations;	NA	NA
3)	Business units.	NA	NA
c)	As parties participating in the origin, amendment, stewardship and use of the health record and whose related actions are ascribed therein:		
1)	Individual healthcare professionals, caregivers;	Yes	NA
2)	Individual authors, scribes and verifiers;	Yes	NA
3)	Organizations;	NA	NA
4)	Business units.	NA	NA
7.2	**Architectural basis**		
7.2.1	**Architectural basis — General**		
7.2.2	**Architectural constructs**		
a)	Data definition:	Yes	Yes
1)	Health record and its subsets;	Yes (subset)	(Yes)
2)	Data groups: datasets, templates;	Yes	Yes
3)	Attributes: data elements;	Yes	Yes
4)	Identifiers;	Yes	Yes
5)	Business objects, relationships;	?	?
6)	Versioning.		
b)	Information model:		
1)	Business classes (objects);	Yes	(Yes)
2)	Subject areas;	Yes	(Yes)
3)	Subject classes (i.e., stateful classes);	Yes	(Yes)
4)	Attributes, identifiers;	Yes	Yes
5)	Relationships between classes, attributes;	Yes	Yes
6)	Vocabulary, coding, classification;	Yes	Yes
7)	Audit;	Yes?	?
8)	Versioning.		

Table A.2 *(continued)*

	Key characteristics	Dept. system to HIS	Device to dept. system
c)	Business operations (process) model:		
1)	Actors (including accountable parties and agents);	Yes	(Yes, devices)
2)	Actions (including accountable actions);	Yes	Yes?
3)	States, state/transitions;	Yes	Yes?
4)	Work flow;	?	?
5)	Audit.	?	?
d)	Information flow model:		
1)	End-to-end:	Yes	Yes
—	Point of origination (point of service/care) to point of use;	Yes	Yes
—	Front-end to back-end to third party;	Yes	?
2)	Stewardship, chain of trust;	?	NA
3)	Audit.	?	NA
e)	Application interoperability model:		
1)	Application role(s);	Yes	Yes
2)	Application interactions: as sender, as receiver;	Yes	Yes
—	Trigger events;	Yes	Yes
—	Unsolicited updates;	Yes	Yes
—	Query/response;	Yes	Yes
—	Receipt acknowledgment;	Yes	Yes?
3)	Inter-application relationships:	Yes	?
—	Point-to-point interaction model: paired sender, receiver roles;	?	?
—	Inter-dependencies;	?	?
4)	Application binding:	?	?
—	API: tightly coupled, passed parameters, delegated control;	Yes	Yes
—	Message: loosely coupled (e.g. ASTM, DICOM, EDI/EDIFACT, HL7, MIB);	Yes	Yes
—	Mediated interchange (e.g. via interface engines, hubs);	Yes	Yes?
i)	En-route queuing, store and forward;	?	NA
ii)	En-route translation, transformation: of data groups, of attributes;	Yes	NA
iii)	Phase I acknowledgement: mediator to transmitter;		
iv)	Phase II acknowledgement: receiver to mediator;		
v)	End-to-end acknowledgement: receiver to transmitter;		
vi)	Phase I threaded message sequence: transmitter to mediator;		
vii)	Phase II threaded message sequence: mediator to receiver;		
viii)	End-to-end threaded message sequence: transmitter to receiver;		
—	Security, access control;	Yes	Yes
—	Audit;	?	?
—	Clock synchrony;	Yes	Yes
—	Data synchrony;	Yes	Yes?
—	Transactions, multi-phase commits (to synchronous data stores);	Yes?	?
—	Data definition;	Yes	Yes

Table A.2 *(continued)*

	Key characteristics	Dept. system to HIS	Device to dept. system
—	Master files;	Yes	?
—	Master registries;	?	?
5)	Versioning.		
f)	Security, Access control model:		?
1)	Access control;	Yes	?
2)	Classifications: for information, function;	Yes	?
3)	Clearances: for users, roles;	Yes	NA
4)	Security policy domains;	Yes	NA
5)	Authentication: user, data source, data verification, data transmittal/receipt;	Yes	NA
6)	Non-repudiation;	?	NA
7)	Digital signature;	Yes	NA
8)	Audit.	?	NA
g)	Accountability model (integral to the Security, Access control model):		
1)	Accountable parties/agents;	Yes?	?
2)	Accountable actions;	Yes?	?
h)	Vocabulary model:	Yes?	Yes
1)	Vocabulary domains;	Yes?	Yes
2)	Coding, classification schemes, including version.	Yes	Yes
7.3	**Master files**		
7.3.1	**Master files — General**		
a)	Synchronize, across 2-n master files:	Yes	NA
1)	At initial application binding;	Yes	NA
2)	Dynamic, in real-time;	Yes	NA
3)	Individual definition instance;	Yes	NA
4)	2-n definition instances;	Yes	NA
5)	All definition instances.	Yes	NA
b)	Find/match definition instance, using matching identifier(s) and/or trait(s);	Yes	NA
c)	Update definition instance, including identifier(s) and/or trait(s) and including actions to: originate, amend/translate;	Yes	NA
d)	Verify definition instance;	Yes	NA
e)	Activate/deactivate definition instance;	Yes	NA
f)	List audit trail for definition instance;	Yes	NA
g)	Update audit trail for definition instance, including actions to: access, originate, amend/translate, verify, transmit, receive;	?	NA
h)	Enable master file transaction, multi-phase commit: bid, open/lock, update, close/unlock;	Yes	NA
i)	Archive definition record(s).		
7.3.2	**Master file: Data definition**		
a)	Health records and subsets thereof:	Yes	
1)	Personal health record: for individual subject of care, health plan member;	Yes	NA
2)	Population health record;	NA	NA
3)	Business (operations) record: for organizations, business units;	NA	NA
4)	Personal service record: for individual healthcare professional, caregiver.	Yes	NA