TECHNICAL REPORT

ISO/TR 21089

First edition
2004-06-01

Health informatics — Trusted end-to-end information flows

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

Reference number
ISO/TR 21089:2004(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.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

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is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.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 document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 21089 was prepared by Technical Committee ISO/TC 215, Health informatics.

Health informatics — Trusted end-to-end information flows

1 Scope

Health(care) records form persistent evidence of health status and the provision and completeness of health(care) services, being retained in electronic and/or other media. Health(care) records often contain Protected Health Information (PHI), typically defined as "individually-identifiable health information", and thus incur safeguards exceeding the ordinary.

The prime unit of health(care) record-keeping is the Entity/Act Record, the authenticatable unit of the health record, evidencing (documenting) the performance/completion of an Act by an Entity and preserving the Accountability Context of the Entity for the Act. (Note that the Entity/Act is central to Health Level Seven's Version 3 Reference Information Model.)

Trusted stewardship, retention and interchange of Entity/Act Records/PHI requires vital safeguards such as traceability and audit. This Technical Report offers an information flow methodology for units of the health(care) record/PHI, particularly the Entity/Act Record, and specifies critical Trace Points (audit events) in that flow including: record/PHI origination, authentication, amendment, translation, access/use, transmittal/disclosure, receipt, de-identification/re-identification, archival, etc.

This Technical Report offers an informative guide to trusted end-to-end information flow for health(care) records and to the key Trace Points and audit events in the electronic Entity/Act Record lifecycle (from point of record origination to each ultimate point of record access/use). It also offers recommendations regarding the trace/audit detail relevant to each.

This Technical Report offers recommendations of best practice for healthcare providers, health record stewards, software developers and vendors, end users and other stakeholders, including patients.

2 References

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

ISO/IEC 2382-8:1998, Information technology — Vocabulary — Part 8: Security

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

ISO/IEC 17799, Information technology — Code of practice for information security management

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
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]

3.4
actor
•with respect to an action •an enterprise object (or entity) that participates in the action
[ISO/IEC 15414]

3.5
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.)

3.6
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.

3.7
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.

3.8
archived (records)
archival (records)
healthcare data saved for later reference or use, possibly off-line
[COACH]

3.9
assurance
grounds for confidence, surety, certitude
grounds for confidence that an entity meets its security objectives
[ISO/IEC 15408-1:1999]

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]

3.10
audit control
mechanisms employed to record and examine system activity

3.11
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 entities) 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]

3.12
authentication of health record entries
process used to verify that an entry is complete, accurate and final
[JCAHO]

3.13
authentication
providing assurance regarding the identity of a subject (author) or object (information)
[ASTM E1762]

3.14
authentication (data)
verification of the integrity of data that have been stored, transmitted or otherwise exposed to possible unauthorized modification
[GCST]

3.15
authentication (data source)
corroboration that the source of data received is as claimed
[ISO 7498-2]

3.16

authentication (user)
provision of assurance of the claimed identity of an entity
[ISO/IEC 10181-2]

3.17
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]

3.18
authorized user
user who may, in accordance with the Security Policy, perform an operation

3.19
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]

3.20
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.

3.21
care
provision of accommodations, comfort and treatment to an individual subject of care (patient), also implying responsibility for safety
[JCAHO]

3.22
caregiver
cf. healthcare professional

3.23
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]

3.24
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

3.25
coding scheme

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

3.26
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]

3.27
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]

3.28
credentials (for identity)
data that are transferred to establish the claimed identity of an entity
[ISO/IEC 2382-8]

3.29
credentials (for healthcare practice)
documented evidence of (a healthcare professional's) licensure, education, training, experience, or other qualifications
[JCAHO]

3.30
criteria
expected level(s) of achievement, or specifications against which performance can be assessed
[JCAHO]

3.31
data attribute, element or item
single unit of data that in a certain context is considered indivisible

3.32
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]

3.33
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]

3.34
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.

3.35
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]

3.36
documentation
process of recording information in the (health) record
[JCAHO]

3.37
electronic health record
EHR
electronic healthcare record
ECHR
health record concerning the subject of care in computer-readable form
[CEN ENV13606-1]

3.38
entity
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]

3.39
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

3.40
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]

3.41
health record
healthcare record
account compiled [by healthcare entities (e.g., 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]

3.42
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]

3.43
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.

3.44
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 ENV12265, modified]

3.45
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]

3.46
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]

3.47
healthcare organization
generic term used to describe many types of organizations that provide healthcare services
[JCAHO]

3.48
healthcare entity
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]

3.49
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.

3.50
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]

3.51
health plan
individual or group plan that provides, or pays the cost of, medical care
[HIPAA]

3.52
identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator
[CEN ENV 13608-1]

3.53
indelible
indelibility
impossible to remove or erase, permanent

3.54
indicator (of performance)
measure used to determine over time, (an organization's) performance of functions, processes and outcomes
[JCAHO]

3.55
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]

3.56
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]

3.57
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]

3.58
integrity (message)
proof that the message content has not altered, deliberately or accidentally in any way, during transmission
[ISO/IEC 7498-2]

3.59
interface
process that permits the flow of data from one system to another in a structured manner

3.60
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

3.61
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]

3.62
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.

3.63
measure
measurement
collect quantifiable data about a function or process
[JCAHO]

3.64
message
logically ordered dataset designed to communicate essential information between systems

3.65
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 2382-8]

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

3.66
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

3.67
organization
unique framework of authority within which a person or persons act, or are designated to act towards the

same purpose

3.68
outcome
result of the performance (or non-performance) of a function or process(es)
[JCAHO]

3.69
patient
cf. subject of care

3.70
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]

3.71
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]

3.72
persistent
persistence
enduring
existing or remaining in the same state for an indefinitely long time

3.73
personal health information
PHI
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]

3.74
personal information
any information relating to an identified or identifiable natural person
[EU Directive 95/46/EC, MEDSEC]

3.75
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]

3.76
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]

3.77
protocol (care)
cf. critical paths

3.78
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]

3.79
registry
server capable of holding data for the systematic and continuous follow up of information objects maintained in accordance with specific rules

3.80
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]

3.81
retention
maintenance and preservation of information in some form (e.g. paper, microfilm, or electronic storage) for a given period of time
[CPRI]

3.82
secondary record
record that is derived from the primary record and contains selected data elements
[ASTM E1384]

3.83
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]

3.84

security (data)
protection of data from intentional or unintentional destruction, modification, or disclosure
[JCAHO]

3.85
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]

3.86
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.

3.87
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.

3.88
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]

3.89
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]

3.90
use (of health information)
sharing, employment, application, utilization, examination, or analysis of such information
[HIPAA]

3.91
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

ACR	American College of Radiologists
ADA	American Dental 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
CMS	Center for Medicare and Medicaid Services, U.S. DHHS
COACH	Canadian Organisation for the Advancement of Computers in Health (now Canadian Health Informatics Association)
CPRI	Computer-Based Patient Record Institute
DHHS	U.S. Department of Health and Human Services
DICOM	Digital Image Communications, ACR/NEMA
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 (now CMS - Center for Medicare and Medicaid Services)
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
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
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)
OMG	Object Management Group
OTA	Office of Technology Assessment (US)
PKC	Public Key Certificate
PKI	Public Key Infrastructure
SDO	Standards Developing Organization
SIG	Special Interest Group
SNIP	Strategic National Implementation Program (for HIPAA), WEDI
TR	ISO Technical Report
USHIK	U.S. Health Information KnowledgeBase, a meta-data registry maintained by the U.S. DHHS (CMS) and DOD, based on ISO 11179
UN	United Nations
WEDI	Work Group for Electronic Data Interchange
WG2	ISO TC215, Working Group 2 on Messaging and Communications

5 Overview - Characteristics Essential to Trusted End-to-End Information Flows

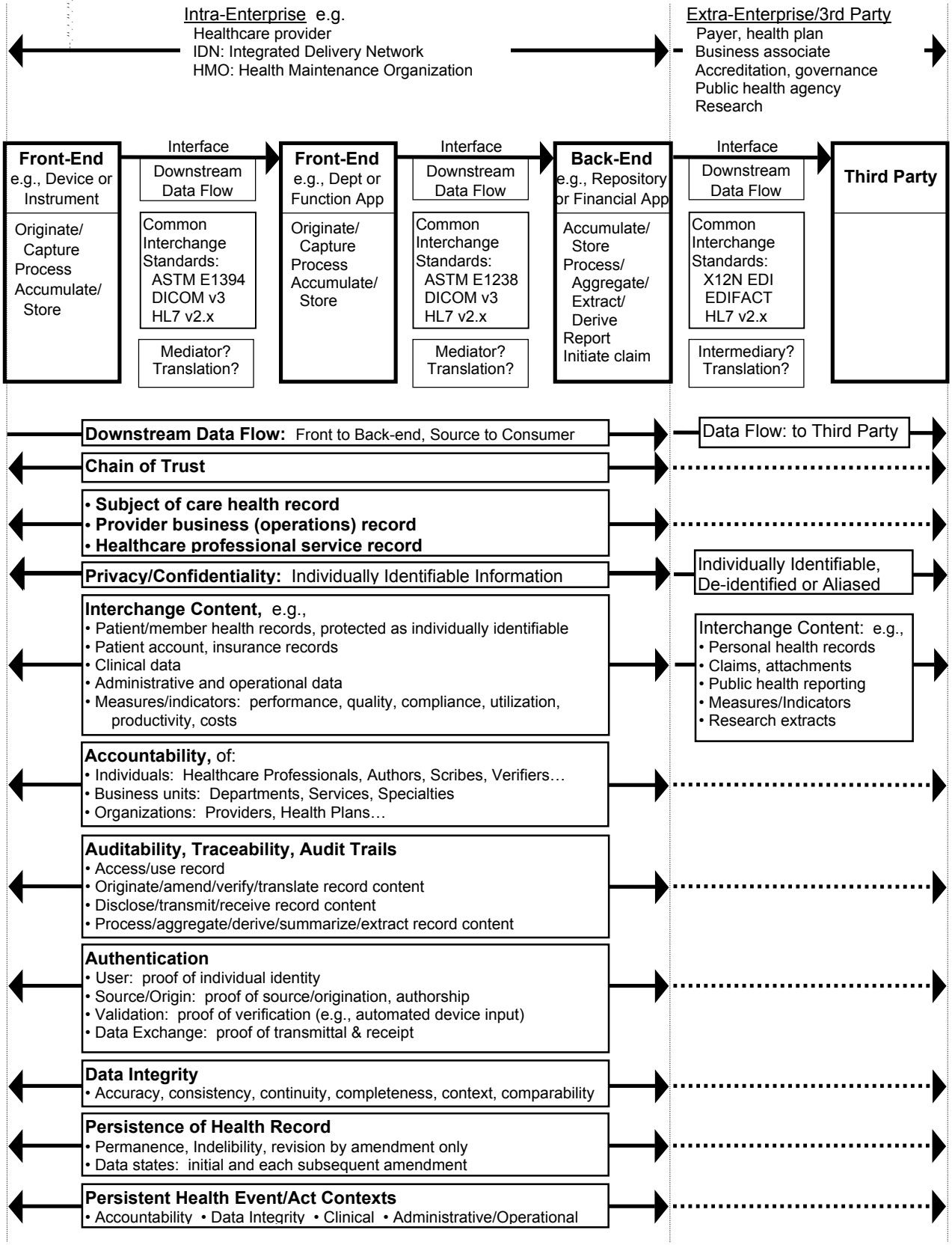


Figure 5.1: Example Scenario for Trusted End-to-End Information Flows

6 Health Record Trust Stakeholders

Health record Trust Stakeholders consist of individuals, organizations and business units. A Trust Stakeholder may be:

6.1 Subject of the health record
6.2 Accountable source or author of health record content
6.3 Accountable verifier of health record content
6.4 Accountable scribe of health record content
6.5 Accountable user of health record content
6.6 Accountable health record steward or keeper
6.7 Accountable provider of health(care) services as ascribed in the health record

Table 6.1 identifies Health Record Trust Stakeholders:

Trust Stakeholders for health record content, including individually identifiable information, protected health information (PHI) Stakeholder	Individual	Organization	Business Unit	Subject of Record	Accountable Source, Author of Record Content	Accountable Verifier of Record Content	Accountable Scribe/Proxy of Record Content	Accountable User of Record Content	Accountable Record Steward	Accountable Provider of Health Services as Ascribed in Record
Subject of Care, Health Plan Member	X			Yes	Yes	A/A	N/A	A/A	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	A/A	Yes	A/A	Yes	No
Department, Service, Specialty			X	Yes	N/A	N/A	N/A	Yes	Yes	Yes
Healthcare Provider	X	X		Yes	N/A	N/A	N/A	Yes	Yes	Yes
Integrated Delivery Network (IDN)		X		Yes	N/A	N/A	N/A	Yes	Yes	Yes
Payment Guarantor, Health Plan, HMO	X	X		A/A	No	No	No	Yes	Yes	No
Value Added Network, Claims Clearinghouse		X		No	No	No	No	Yes	Yes	No
Employer	X	X		A/A	No	No	No	Yes	A/A	No
Public Health Agency		X		No	No	No	No	Yes	A/A	No
Regulatory Agency		X		No	No	No	No	Yes	A/A	No
Accreditation Agency		X		No	No	No	No	Yes	A/A	No
Research	X	X		No	No	No	No	Yes	A/A	No
Professional Education	X	X		No	No	No	No	Yes	A/A	No
Others										

N/A = Not applicable, A/A = As applicable

Table 6.1: Trust Stakeholders (in terms of health record content)

[Health Record Trust Stakeholders are consistent with Health Record Trust Constituency members identified in ISO 18307, "Health informatics - Interoperability and compatibility in messaging and communications standards - Key characteristics".]

7 Principles and Objectives

[These Principles are intentionally coincident with ISO 18307, "Health informatics - Interoperability and compatibility in messaging and communications standards - Key characteristics".]

The vital foundation for trusted end-to-end flows for health information is the recognition, promotion and fulfillment of essential principles and objectives, including:

7.1. Ensured Trust

Stakeholders - individuals, organizations and business units - have a trust stake with regard to the integrity and authenticity of the health record, including its origin, amendment, stewardship and use, and with particular regard to:

7.1.1. Privacy and confidentiality;
7.1.2. Protection of individually identifiable information;
7.1.3. Protection during the course of interchange - “in transit”.

7.2. Trust Stakeholders

[Refer also to Section 6, Health Record Trust Stakeholders.]

There are many stakeholders to the health record and its content, each with definitive rights and obligations:

7.2.1 As subjects of the health record and whose identity is ascribed in the health record, e.g.:
- 7.2.1.1. Individual subjects of care, health plan members;
- 7.2.1.2. Individual healthcare professionals, caregivers;
- 7.2.1.3. Individual originators of record content: authors, scribes/proxies and verifiers;
- 7.2.1.4. Organizations, including: providers, health plans;
- 7.2.1.5. Business units, including: departments, services, specialties;
- 7.2.1.6. Others, including: next of kin, emergency contacts, payment guarantors;

7.2.2. As entities participating in the provision, performance and completion of healthcare services and whose related actions are ascribed in the health record, e.g.:
- 7.2.2.1. Individual healthcare professionals, caregivers;
- 7.2.2.2. Organizations;
- 7.2.2.3. Business units;

7.2.3. As entities participating in the origin, amendment, stewardship and use of the health record whose related actions are ascribed therein, e.g.:
- 7.2.3.1. Individual healthcare professionals, caregivers;
- 7.2.3.2. Individual authors, scribes/proxies and verifiers;
- 7.2.3.3. Organizations;
- 7.2.3.4. Business units.

Specific rights and obligations of stakeholders, 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.

7.3. 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:

7.3.1. Confidentiality and privacy protections, particularly with regard to access to, use and disclosure of:
- 7.3.1.1. Individually identifiable information;
- 7.3.1.2. Information subject to protection:
  - 7.3.1.2.1. by statute, regulation, standard of practice or custom; and/or
  - 7.3.1.2.2. by virtue of explicit disclosure grants and agreements;
- 7.3.1.3. Information made available by such grants and agreements:
  - 7.3.1.3.1. for purpose(s) intended;
  - 7.3.1.3.2. by those entities so authorized;
  - 7.3.1.3.3. for the period (of time) designated; and
  - 7.3.1.3.4. based on the principle of “need to know”.

7.3.2. Complete and accurate portrayal of health status and interventions;
7.3.3. Complete and accurate portrayal of the provision, performance and completion of health services;
7.3.4. 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.

7.4. Health Record Obligations

Health record obligations include accountability for:

7.4.1. Record content origination and amendment, as ascribed to authors, scribes/proxies and/or verifiers;

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

7.4.3. Accuracy, completeness of record content;

7.4.4. Access to, and use of, record content;

7.4.5. Duplication of record content;

7.4.6. Disclosure, transmission and receipt of record content;

7.4.7. 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.

7.5. Health Record Composition

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

7.5.1. A longitudinal chronology of health status and interventions;

7.5.2. A chronicle of health service events/acts corresponding to the provision, performance and completion of healthcare services;

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

7.6. Healthcare Entities and Their Accountable Actions

Healthcare entites are those individuals, organizations and business units accountable for actions (conscious acts) related to, and/or ascribed in, the health record, including:

7.6.1. Origination or amendment of record content: as authors, scribes/proxies, verifiers;

7.6.2. Provision, performance and/or completion of healthcare services, specifically health service events/acts;

7.6.3. Access to, and use of, record content;

7.6.4. Duplication of record content;

7.6.5. Disclosure, transmission and/or receipt of record content;

7.6.6. Translation of record content.

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

7.7. 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:

7.7.1. Origination of record content (typically pre-verification);

7.7.2. Duplication of record content;

7.7.3. Transmission and/or receipt of record content;

7.7.4. Translation of record content.

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

7.8. Scope of Accountability, Unit of Accountability

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

7.8.1. Healthcare entities in terms of their specific actions in the provision, performance and/or completion of health services;

7.8.2. Healthcare entities 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):

7.8.3. Describing the performance, provision and/or completion of a discrete health service event/act;
7.8.4. Comprising a discrete record instance.

7.9. Authentication

Authentication is fundamental to the trusted interchange of healthcare information. It enables a recipient to reliably verify the entities responsible for the origination, validation, transmittal and receipt of health records, in whole or in part. Specific authentication functions are crucial, these include:
7.9.1. User authentication: evidence of individual identity;
7.9.2. Data source/origin authentication: evidence of authorship, origination, amendment;
7.9.3. Data validation authentication: evidence of data verification, e.g.:
7.9.3.1. of data originated by another entity;
7.9.3.2. of automated device input;
7.9.4. Data interchange authentication: evidence of data transmittal, receipt.

Additional aspects of authentication include:
7.9.5. Non-repudiation (e.g., of authorship);
7.9.6. Digital signature;
7.9.7. Public/private key infrastructure;
7.9.8. Encrypted encapsulation: binding record content to an authenticated source.

7.10. Auditability

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

7.11. 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.

7.12. Faithfulness, Permanence, Persistence and Indelibility

Another pre-requisite 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:
7.12.1. Preservation of original content and context;
7.12.2. Revision by (additive) amendment only;
7.12.3. Preservation of discrete data states: for the original and each amendment;
7.12.4. Ability to reconstruct health records for any given historical date/time.

7.13. 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 data sets). 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.

7.14. Data Integrity

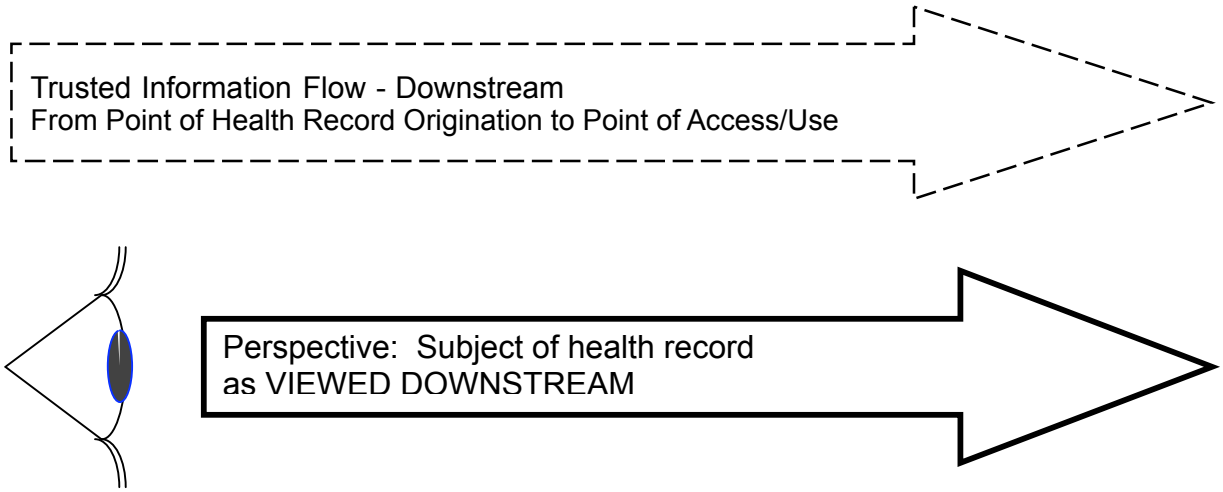
Significant aspects of data integrity include accuracy, context, consistency, comparability, continuity, completeness and relevance. Data integrity is based on data definition, as described above, but also relies substantially on robust methods for information flow from the point of origination to the point of use.

7.15. Completeness

Completeness constitutes a prime objective, specifically the requirement to ensure completeness in:
7.15.1. process of healthcare delivery, including the completeness of discrete events/acts, encounters and episodes;
7.15.2. health records, including its correlative documentation of the health delivery process;
7.15.3. 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.

8 Information Flow Perspectives

8.1 Downstream Perspective - Health Record Subject



As the health record subject (e.g., patient, health plan member)…

How might I be assured of (trust) the persistent integrity and authenticity of my health record and its content?

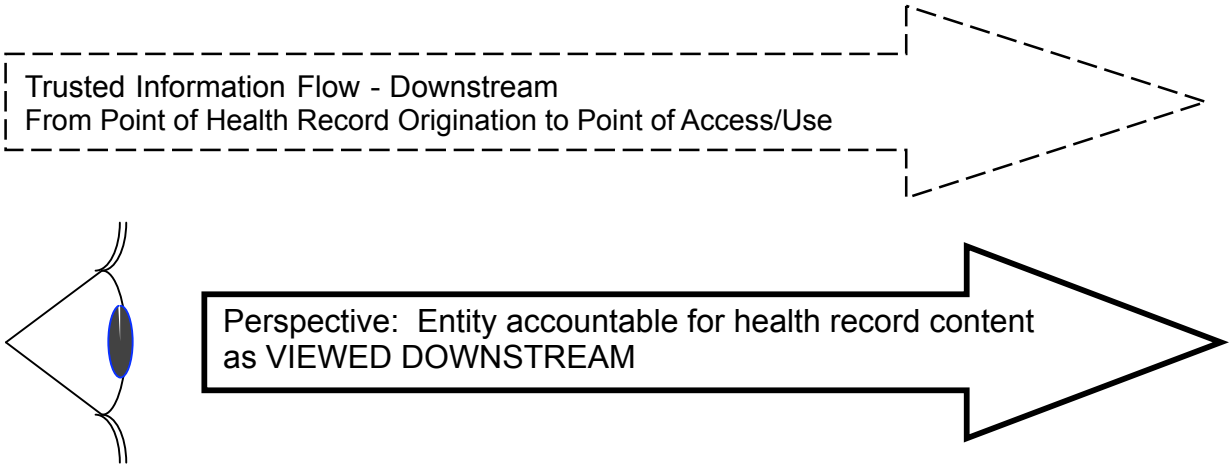
How might I be assured that access/use of my health record is based on "need to know"?

How might I be assured that routine access/use of my health record is according to my consent agreement? Other disclosures according to my specific authorization?

With regard to my health record, how might I be assured (trust) that accountable actions by accountable parties are ascribed, authenticated and traceable, including key points in the record lifecycle:

- Record origination, amendment, verification, translation?
- Record access/use?
- Record disclosure and transmittal?
- Record receipt, retention and stewardship?
- Record de-identification or aliasing?
- Record archival, loss or destruction?
- Physical record check-out/in?

8.2 Downstream Perspective - Entity(ies) Accountable for Health Record Content



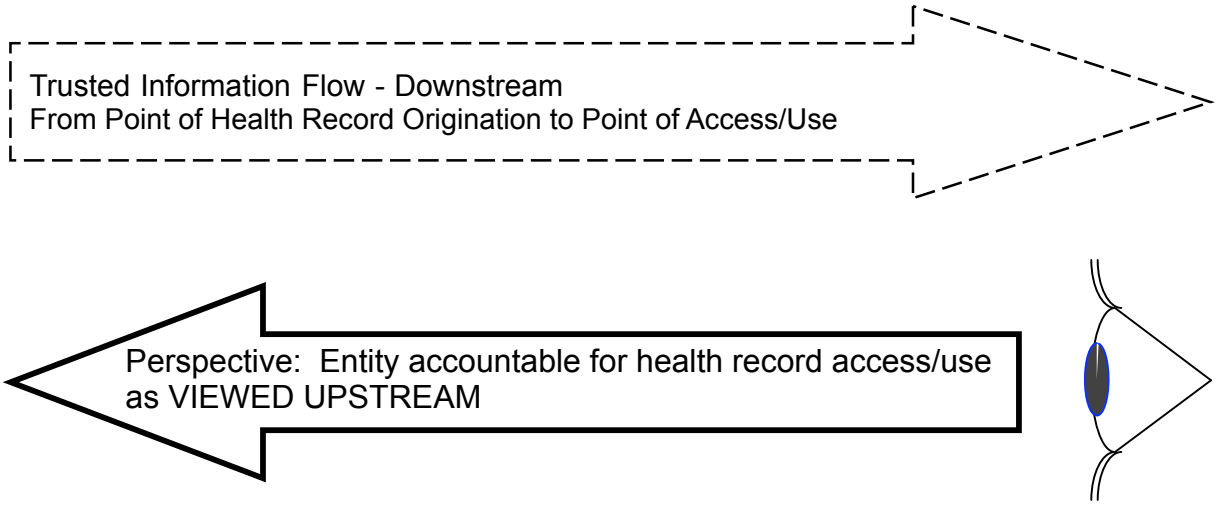
As an accountable provider of health(care) services (as ascribed in the health record)…
As an accountable author, scribe and/or verifier of health record content…

How might I be assured of (trust) the persistent integrity and authenticity of health record content ascribed to me?

With regard to health record content ascribed to me, how might I be assured (trust) that subsequent accountable actions by accountable parties are ascribed, authenticated and traceable, including key points in the record lifecycle:

- Record origination, amendment, verification, translation?
- Record access/use?
- Record disclosure and transmittal?
- Record receipt, retention and stewardship?
- Record de-identification or aliasing?
- Record archival, loss or destruction?
- Physical record check-out/in?

8.3 Upstream Perspective - Entity(ies) Accountable for Health Record Access/Use



As an accountable user of health record content…

How might I be assured of (trust) the persistent integrity and authenticity of health record content which I access and use?

With regard to health record content, how might I be assured (trust) that accountable actions by accountable parties are ascribed, authenticated and traceable, including key points in the record lifecycle:

- Record origination, amendment, verification, translation?
- Record access/use?
- Record disclosure and transmittal?
- Record receipt, retention and stewardship?
- Record de-identification or aliasing?
- Record archival, loss or destruction?
- Physical record check-out/in?

9 Entities, Health Service Acts and Corresponding Persistent Act Records

1 Act Performance

Entity performs Health Service Act

- Entity is
  - Individual: e.g., healthcare professional, health record user
  - Organization: e.g., healthcare provider, health plan
  - Business unit: e.g., department, service, specialty
- Act performed is a health service action or event: e.g., a care action, a diagnostic or therapeutic procedure, an observation
- Act performed may be related to an individual subject of care (i.e., patient), or not
- Act performance constitutes a discrete work flow event and may include attributes for assignment, status and completeness
- Act performed may be:
  - A single discrete instance (standing alone); or
  - Closely associated with other Health Service Act(s): e.g., the set of Acts necessary to fulfill an order
- Act as performed may transition through multiple states: e.g., from scheduled/pending, to assigned, to "in progress", to complete/fulfilled
- Act performance is traceable from initiation through each subsequent state transition

2 Act Documentation

Entity documents (performance of) Health Service Act in corresponding Act Record

- Documenting Entity may (or may not) be the same as Performing Entity
- Act Record is persistent evidence of the Entity/Act
- Act Record is legal evidence of Entity/Act subject of care, care provider, date/time of service/care, type of service/care rendered, duration and location of service/care
- If Act is subject of care (patient) related, Act Record is individually identifiable and thus constitutes Protected Health Information (PHI)
- Act Record may be authenticated by its author/source and/or verifier
- Act Record evidences key Act Contexts: Accountability, Data Integrity, Clinical, Administrative/Operational
- Act Record has traceable versioning: from origination, through each subsequent amendment (and thus retains original and each successive data state)
- Act Record has traceable flow, from point of origination onward

3 Persistent Act Record

Entity stewards the Persistent Act Record

- Persistent Act Record is enduring and traceable (auditable) from its point of origination onward
- Persistent Act Record includes evidence of accountability, authentication, audit trails, data integrity, persistence, retention
- Persistent Act Record is versioned, from original through each amendment, fully preserving each successive data state
- Persistent Act Record is retained by the originating Entity (typically) at least for the minimum legal period
- Persistent Act Record includes evidence at points of traceability (audit), specifically: origination, amendment, verification, translation, access/use, transmittal/disclosure, receipt, reporting, archival, destruction or loss, de-identification/re-identification

10 Health Service Act - Vital Contexts - as documented in the Act Record

Trusted end-to-end information flows convey Health Service Act(s) and their vital contexts, as documented in the Act Record, from the point of origination (e.g., point of service/care) to any ultimate point of record access/use where such contexts ensure completeness and integrity.

10.1. Accountability Context

Describes the essential who, what, when, where and why aspects of the performance, provision and completion of health service acts and the origination, amendment, stewardship and use of health records. It ensures the ascription of accountable entities to their accountable actions.

10.2. Data Integrity Context

Describes essential data integrity aspects relevant to the content of a health service act record and includes measures and indicators for (as applicable): accuracy, context, consistency, comparability, continuity, completeness and relevance.

10.3. Clinical Context

Describes essential clinical frame of reference relevant to a health service act and thus to the content of its corresponding act record and includes (as applicable):

10.3.1. Rationale;
10.3.2. Clinical parameters;
10.3.3. Clinical context and conditions;
10.3.4. Rules and measures to ensure:
- 10.3.4.1. continuity and completeness;
- 10.3.4.2. compliance: e.g., with standards of practice/care;

10.3.5. Measures and indicators: e.g.,
- 10.3.5.1. performance;
- 10.3.5.2. quality;
- 10.3.5.3. outcomes.

10.4. Administrative/Operational Context

Describes the essential administrative/operational frame of reference relevant to a health service event/act and thus to the content of its corresponding health record instance and includes (as applicable):

10.4.1. Allocation, deployment: e.g., of resources;
10.4.2. Assigned responsibility: e.g., of healthcare entities;
10.4.3. Parameters and measures: e.g.,
- 10.4.3.1. resource utilization: staff, facilities, equipment, supplies, time;
- 10.4.3.2. costs;
- 10.4.3.3. productivity, work load.

11 Roles and Relationships (Example)

11.1. Subject of Care and Providers

These roles instantiate the relationship between the subject of care and his/her health care providers (including individual healthcare professionals and caregivers) and relate:

11.1.1. Subject of care (e.g., patient, health plan member);
11.1.2. Providers, healthcare professionals, caregivers, e.g.:
    11.1.2.1. Usual, primary physician;
    11.1.2.2. Admitting, attending physician;
    11.1.2.3. Consultant;
    11.1.2.4. Nurse;
    11.1.2.5. Therapist;
    11.1.2.6. Home caregiver;
11.1.3. Others: next of kin, emergency contact(s), guarantor(s).

11.2. Health Services

These roles instantiate the relationship of individual healthcare professionals and caregivers to the provision, performance and completion of health services and include:

11.2.1. performer of;
11.2.2. observer of.

11.3. Health Record

These roles instantiate the relationship of individuals, organizations and business units to the origination, amendment, stewardship and use of health records, including:

11.3.1. origination, amendment of: author, scribe/proxy;
11.3.2. verifier of: e.g., content authored by another, input from automated device;
11.3.3. access to and use of;
11.3.4. stewardship of;
11.3.5. duplication of;
11.3.6. disclosure, transmission and/or receipt of;
11.3.7. translation of.

11.4. Individuals, Organizations, Business Units

These roles instantiate the relationship among and between individuals, organizations and business units and include:

11.4.1. business units as operational components of an organization: e.g., departments, services and specialties which are discretely managed, functional parts of a healthcare provider organization;
11.4.2. individuals vis-à-vis an organization and/or business unit, acting:
    11.4.2.1. as an employee/agent of; and/or
    11.4.2.2. on behalf of.

11.5. Inter-Healthcare Professional

These roles instantiate the relationship among and between individual healthcare professionals, caregivers, including:

11.5.1. chief to resident;
11.5.2. preceptor, proctor, instructor to student;
11.5.3. supervisor to staff.

12 Key Definition and Trace/Audit Points in Trusted End-to-End Information Flows

12.1. Act Record - Point of Definition, of:

- Data attributes: e.g., data elements
- Data groups: e.g., datasets
- Context sets, templates: specialized data groups recording the vital context of health service events/acts
- Health record: a composition documenting one or more health service events/acts

12.2.1. Health Service Act - Point of Service/Care
12.2.2. Act Record - Point of Origination

12.3.1. Health Service Act - Point of Progression or Completion
12.3.2. Act Record - Point of Amendment

12.4. Act Record - Point of Translation

12.5. Act Record - Point of Access/Use

12.6.1. Act Record - Point of De-Identification, Aliasing
12.6.2. Act Record - Point of Re-identification

12.7. Act Record - Point of Convergence: e.g., aggregation, summarization or derivation

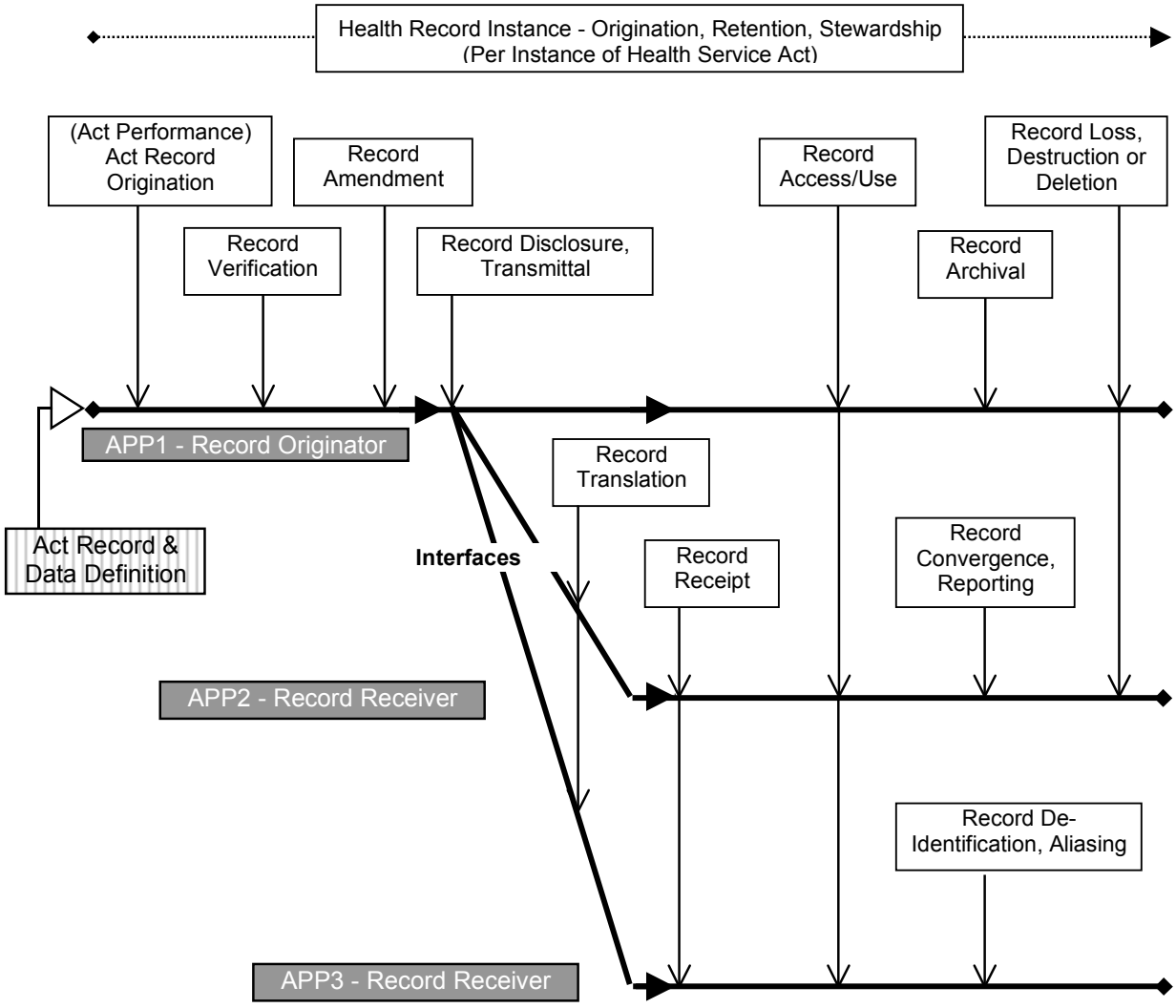
12.8.1. Act Record - Point of Disclosure, Transmittal
12.8.2. Act Record - Point of Reporting

12.9. Act Record - Point of Receipt

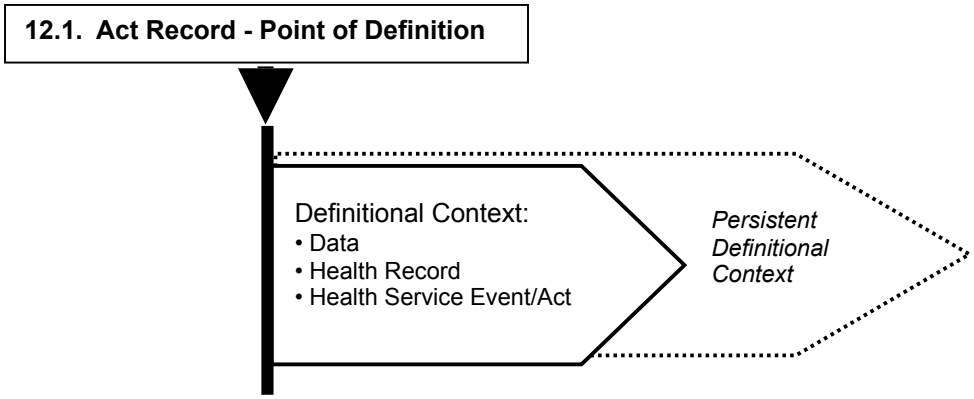
12.10. Act Record - Point of Archival

12.11. Act Record - Point of Loss, Destruction or Deletion

Figure 12.1 Key Trace/Audit Points in Trusted End-to-End Information Flow (Example)

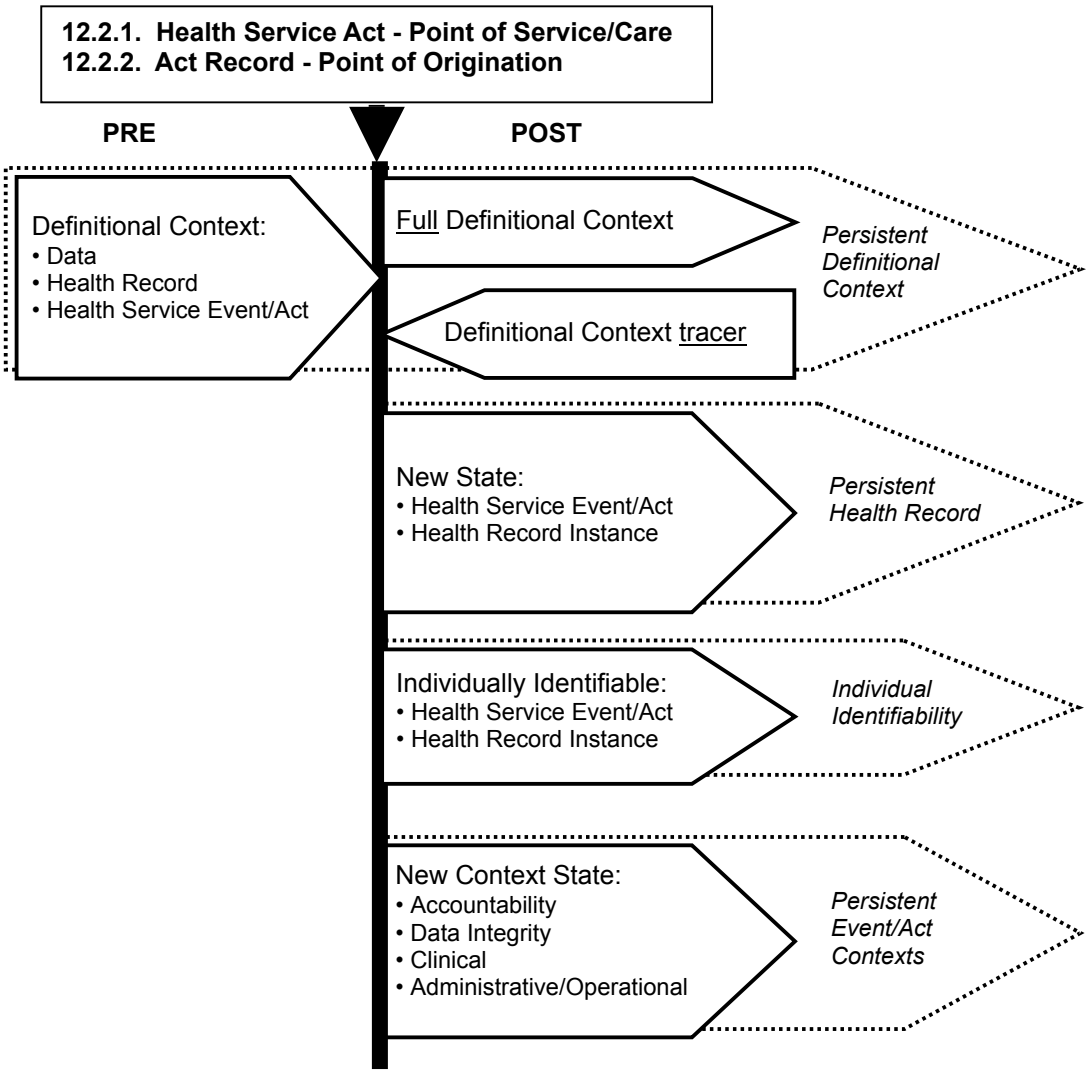


12.1. Act Record - Point of Definition	**Attribute Definition** (e.g., atomic data elements) For each: 1. Attribute Instance ID 2. Name, description 3. Precise usage 4. Data type, format 5. Classification, coding scheme (if any) 6. Range 7. Data attribute integrity: measures and rules for accuracy, consistency, comparability, continuity, completeness **Data Group Definition** (e.g., datasets) For each: 1. Data Group Instance ID 2. Name, description 3. Precise usage 4. Aggregated attributes 5. Data group integrity: contextual (attribute) relationships, measures and rules for consistency, comparability, continuity, completeness **Context Sets** Persistent in terms of trusted information flow: from point of record/data origination to point of use Specialized data groups forming the vital context of health service events/acts: 1. Accountability context 2. Data integrity context 3. Clinical context 4. Administrative/operational context



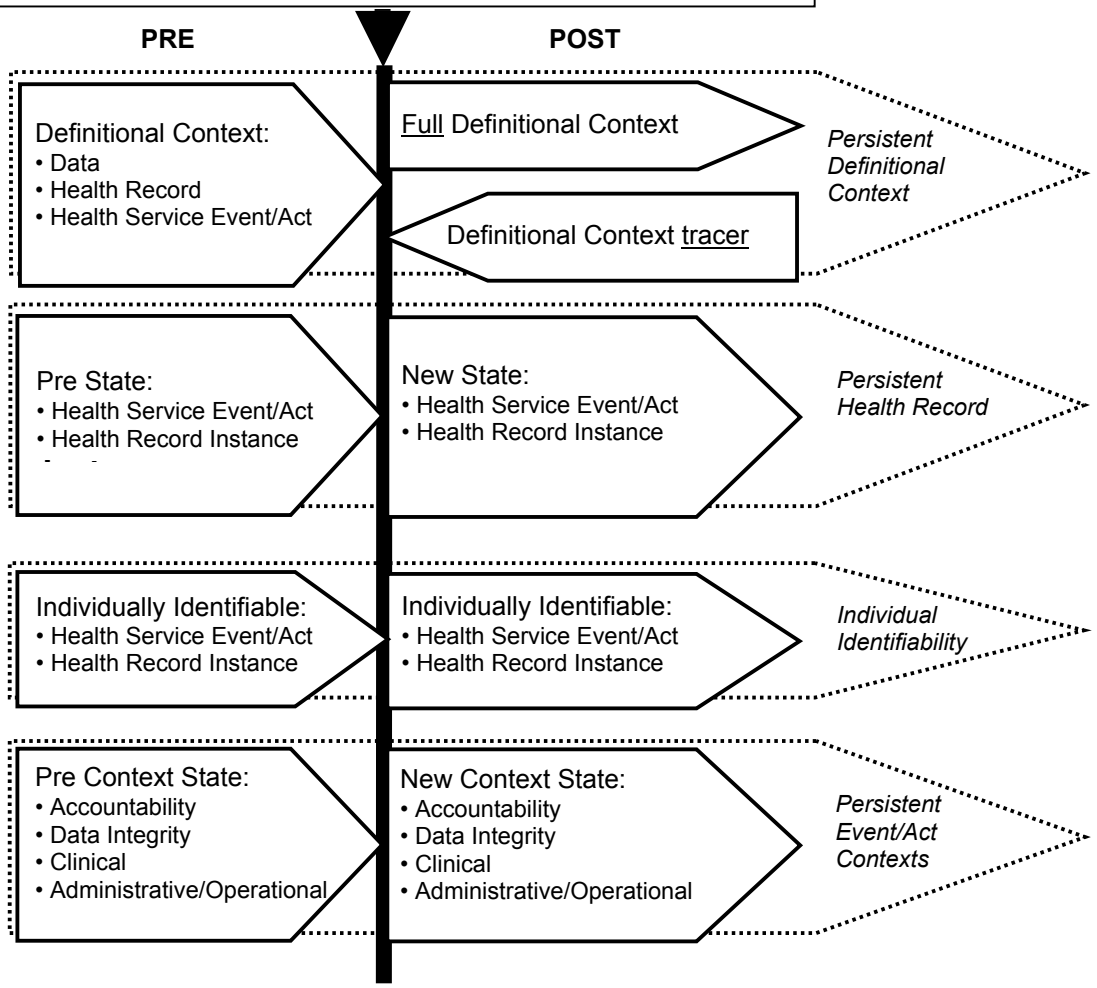
12.2.1. Health Service Act - Point of Service/Care	**Accountability Context** Service Event/Act Instance ID Who - Event/Act Subject - Individual Subject of Care ID Who - Accountable Healthcare Entity(ies), as pertains to each: <Digital Signature> Organization ID/Descriptor, if applicable Business Unit ID/Descriptor, if applicable Individual Healthcare Professional, Caregiver ID Role - relative to organization, business unit Role - relative to patient/member Role - relative to service event/act instance Role - relative to individual performer Scope of accountability What - service event/act performed, rendered: service ID What - action: perform, assist, observe What - service event/act status: pending, in progress, complete, canceled What - corresponding health record instance When - service event/act date/time, duration Where - physical location: point of service/care Where - network address, device ID Why - rationale, as applicable **Data Integrity Context** Measures, rules and indicators to ensure, as applicable: data accuracy, context, consistency, comparability, continuity, completeness, relevance **Clinical Context** As applicable: • Rationale • Clinical parameters • Clinical context, conditions • Measures and rules to ensure continuity, completeness (e.g., of the clinical service event/act) • Measures and indicators for compliance (e.g., with standards of practice/care), quality, performance, outcomes **Administrative/Operational Context** As applicable: • Allocations, deployments • Assigned responsibility • Resource utilization: staff, time, facilities, equipment, supplies • Costs • Productivity, work load

12.2.2. Act Record - Point of Origination	**Accountability Context** Record Instance ID Who - Record Subject - Individual Subject of Care ID Who - Accountable Healthcare Entity(ies), as pertains to each: <Digital Signature> Organization ID/Descriptor, if applicable Business Unit ID/Descriptor, if applicable Individual Healthcare Professional, Caregiver ID Role - relative to organization, business unit Role - relative to record instance Role - relative to individual author, verifier Scope of accountability What - record type (e.g., document type) What - action: author, scribe/proxy, verifier What - record instance status: new, amended, verified What - record completion status: documented, dictated (pre-transcription), in progress, incomplete, pre-authenticated, authenticated, legally authenticated (ref: HL7) What - related health service event/act ID When - recording date/time, duration Where - physical location: point of recording Where - network address, device ID Why - rationale, as applicable Who - Accountable Healthcare Agent(s), as pertains to each: Device, application or software ID Role, relative to record instance: originator Scope of accountability What - action: originate What - related healthcare service When - date/time of origination Where - physical location Where - network address **Data Integrity Context** Measures, rules and indicators to ensure, as applicable: data accuracy, context, consistency, comparability, continuity, completeness, relevance **Clinical Context** **Administrative/Operational Context** As encapsulated in corresponding health service event/act

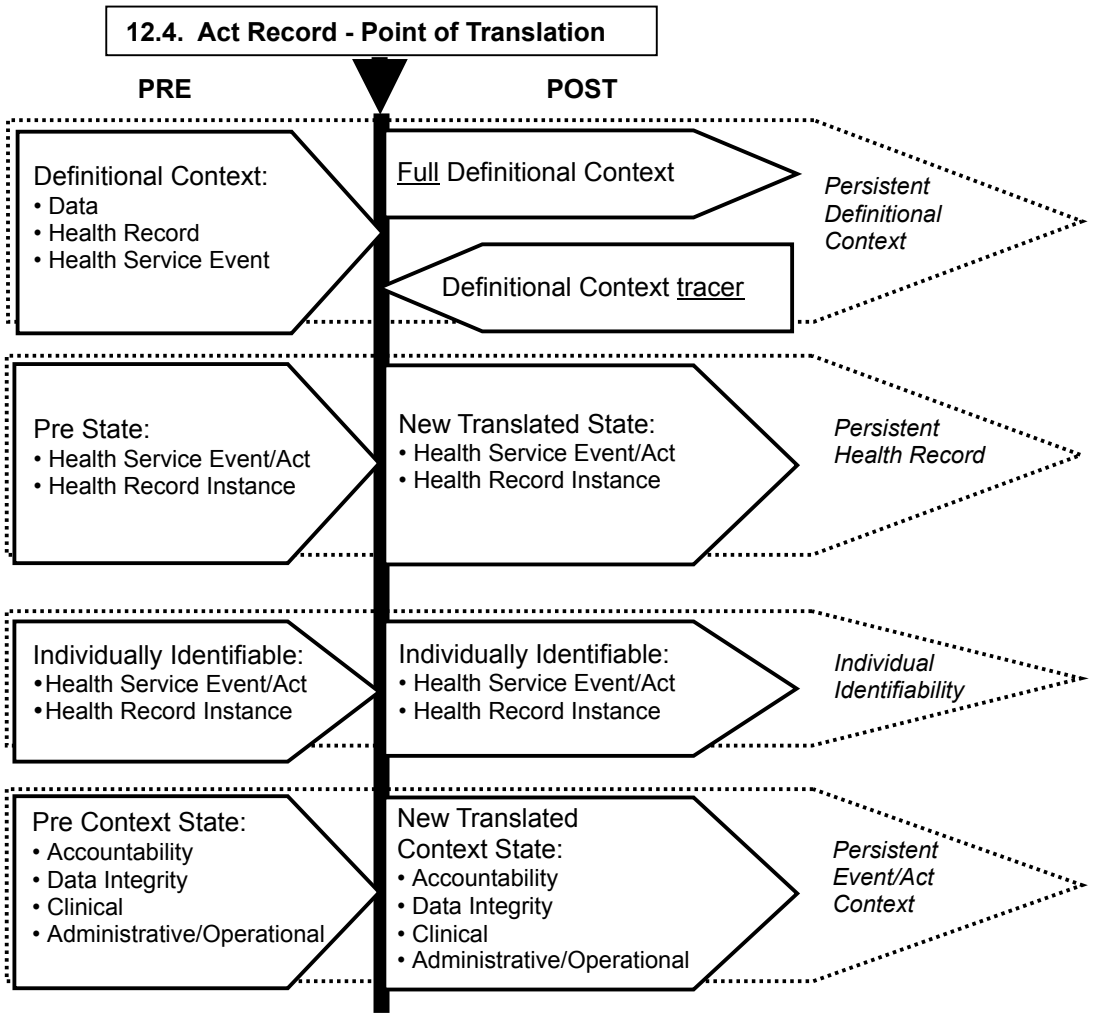


12.3.1. Point of Progression or Completion: **Health Service Event/Act**	SAME as 12.2.1, except: • Preserve health service event/act pre-state • Append health service event/act post-state as amendment Carry forward full or traceable health service event/act contexts: • Accountability • Data Integrity • Clinical • Administrative/Operational
12.3.2. Point of Record/Data Amendment **Health Record Instance**	SAME as 12.2.2, except: • Preserve health record instance pre-state • Append health record instance post-state as amendment Carry forward full or traceable health service event/act contexts: • Accountability • Data Integrity • Clinical • Administrative/Operational

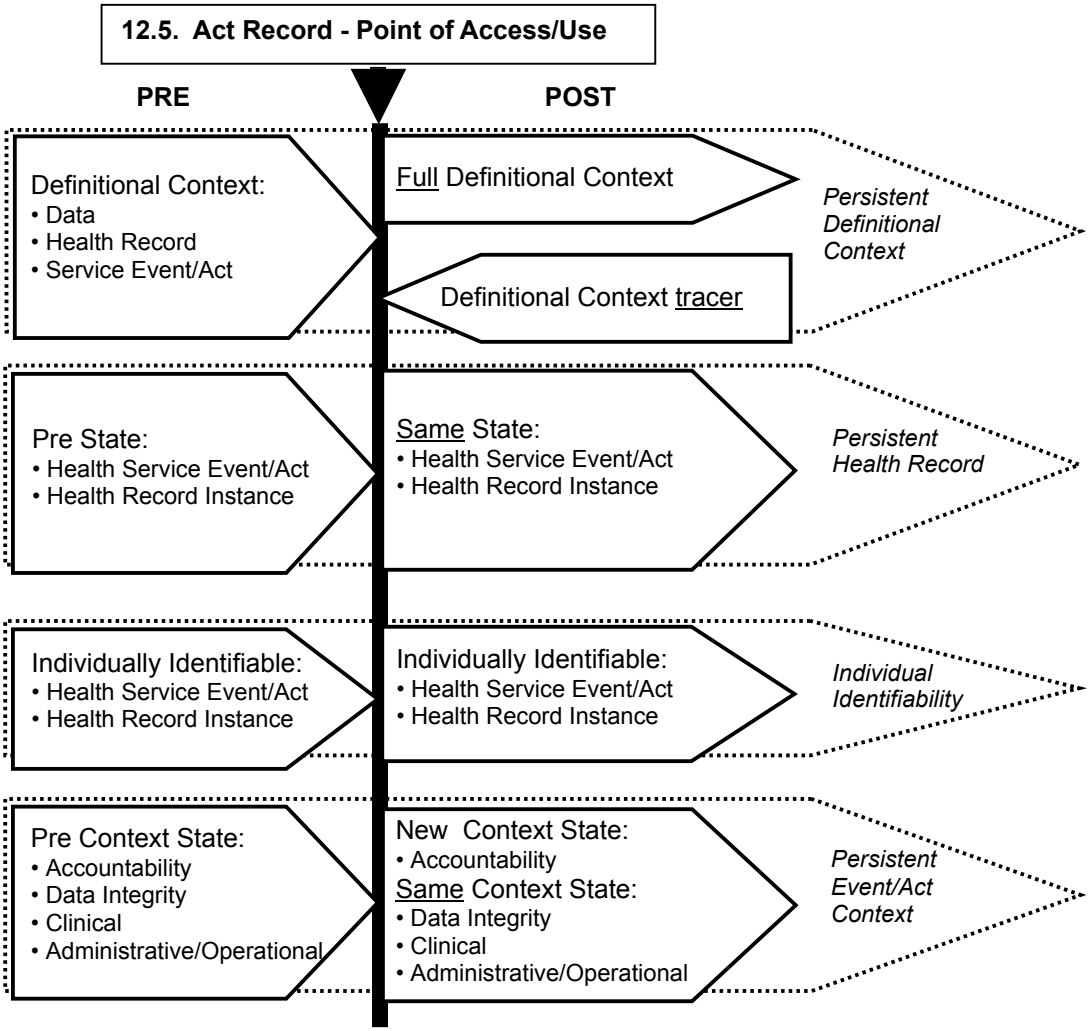
12.3.1. Health Service Act - Point of Progression or Completion
12.3.2. Act Record - Point of Amendment



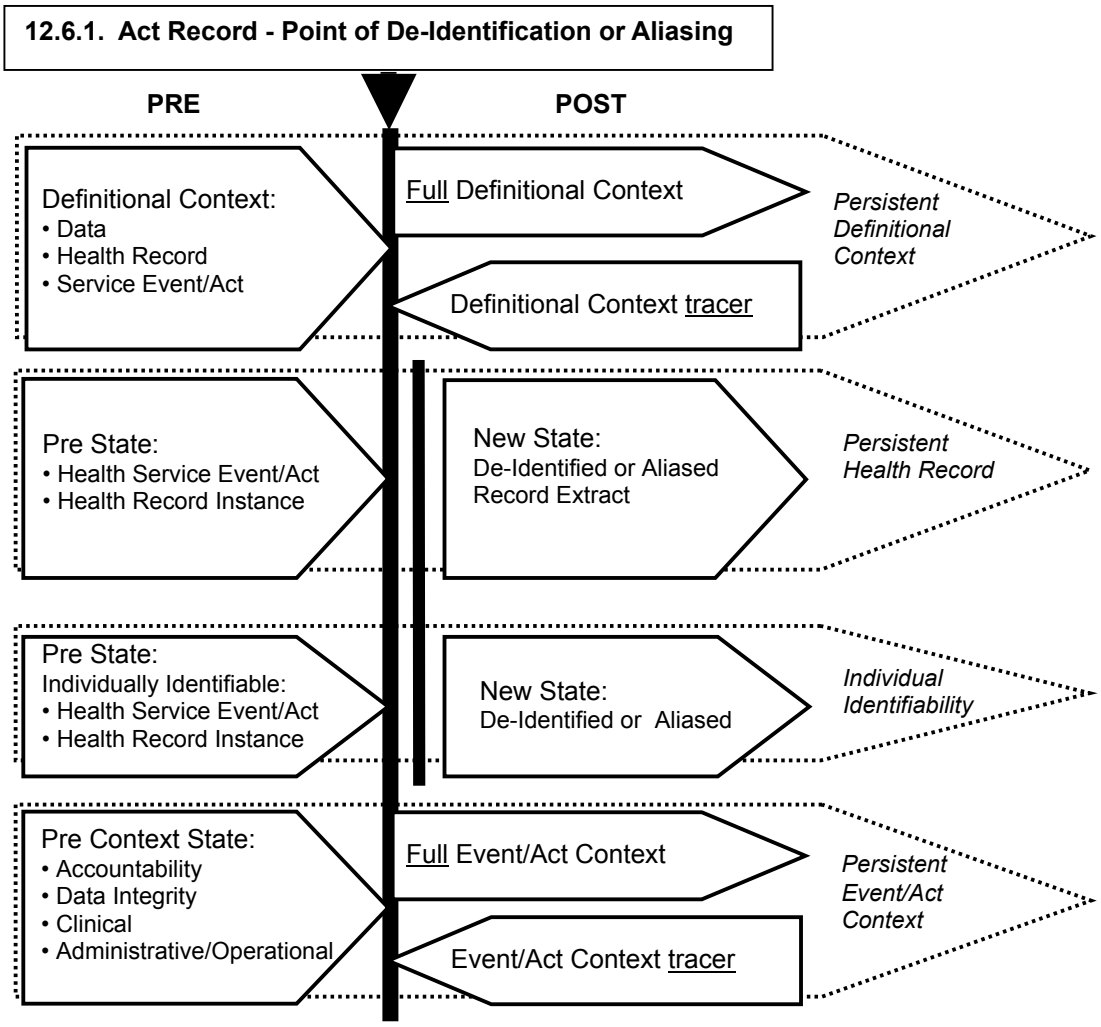
12.4. Act Record - Point of Translation	• Preserve health record instance pre-state • Append health record instance post-state as amendment **Accountability Context**, for this translation: Record Instance ID Who - Record Subject - Individual Subject of Care ID Who - Accountable Healthcare Agent(s), as pertains to each: <Digital Signature> Device, application or software ID Role, relative to record instance: mediator, translator Scope of accountability What - action: translate When - date/time of translation Where - physical location Where - network address Carry forward, for this translation, health service event/act contexts: • Accountability • Data Integrity • Clinical • Administrative/Operational



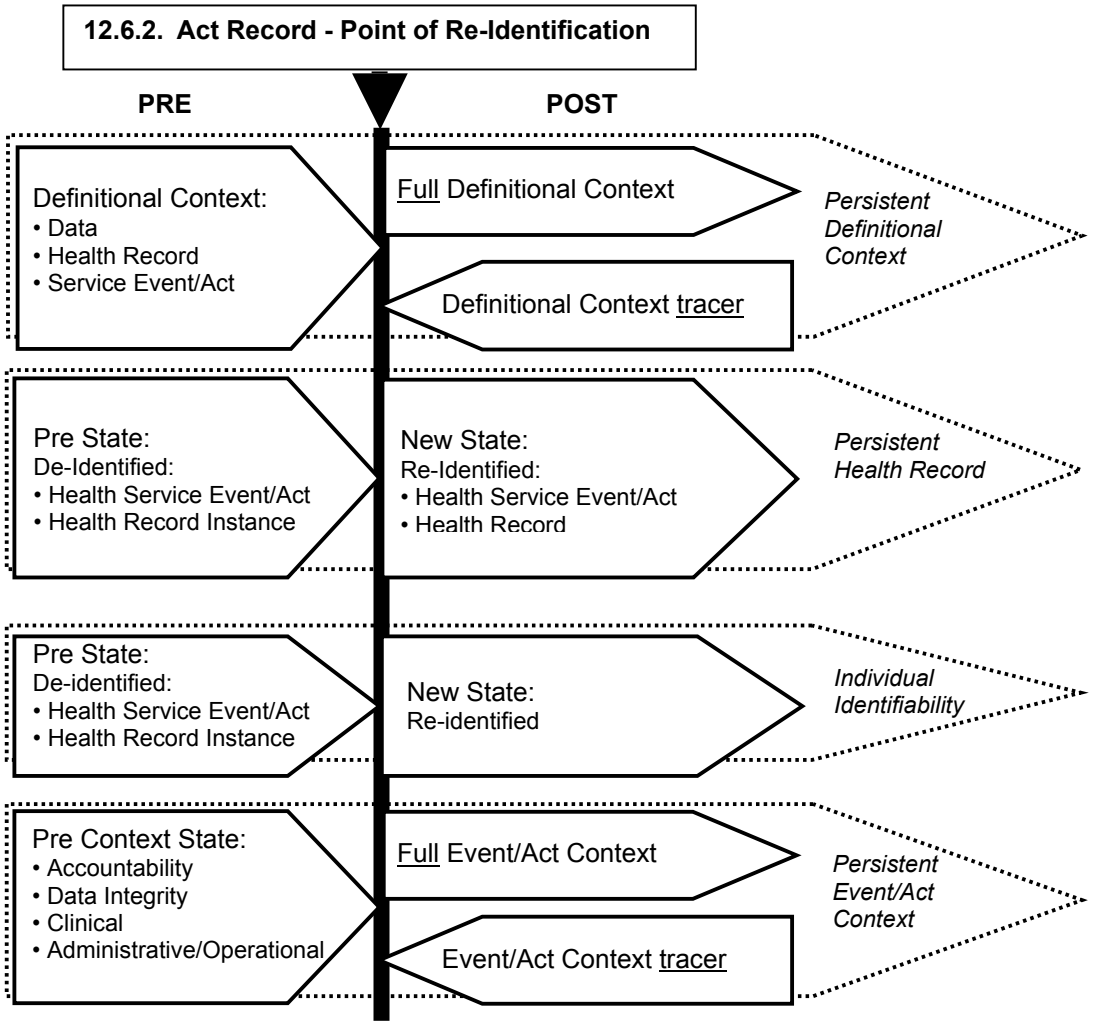
12.5. Act Record - Point of Access/Use	**Accountability Context**, for this access/use: Record Instance ID Who - Record Subject - Individual Subject of Care ID Who - Accountable Healthcare Agent(s), as pertains to each: <Digital Signature> Device, application or software ID Role, relative to record instance: access, use Scope of accountability What - action: access, use When - date/time of access/use Where - physical location Where - network address



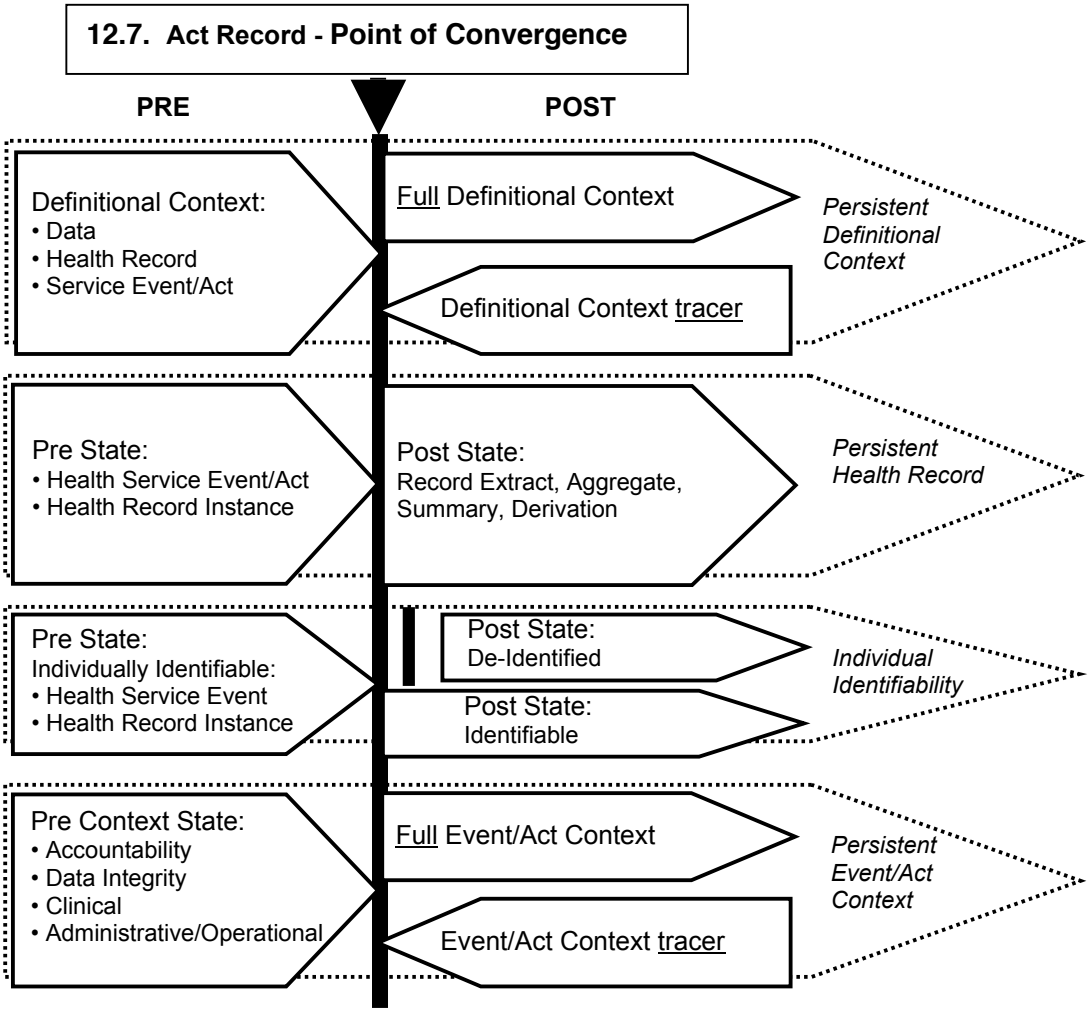
12.6.1. Act Record - Point of De-Identification or Aliasing	• Preserve health record instance pre-state • Append health record instance post-state as amendment **Accountability Context**, for this De-Identification or Aliasing: Record Instance ID Who - Accountable Healthcare Agent(s), as pertains to each: <Digital Signature> Device, application or software ID Role, relative to record instance: de-identification, aliasing Scope of accountability What - action: de-identification, aliasing When - date/time of de-identification, aliasing Where - physical location Where - network address Carry forward full or traceable event/act contexts: • Accountability • Data Integrity • Clinical • Administrative/Operational



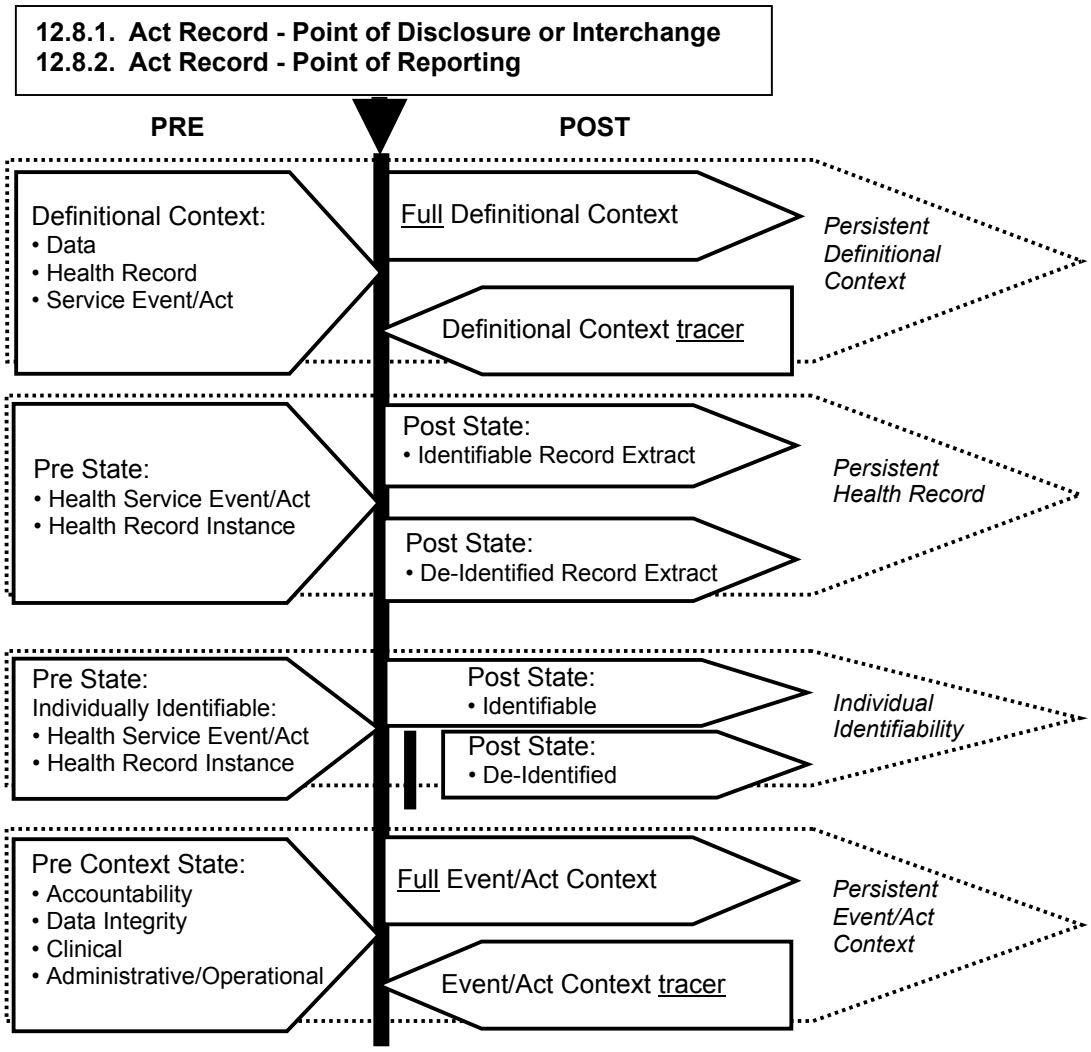
12.6.2. Act Record - Point of Re-Identification	• Preserve health record instance pre-state • Append health record instance post-state as amendment **Accountability Context**, for this Re-Identification: Record Instance ID Who - Accountable Healthcare Agent(s), as pertains to each: <Digital Signature> Device, application or software ID Role, relative to record instance: de-identification, aliasing Scope of accountability What - action: re-identification When - date/time of re-identification Where - physical location Where - network address Carry forward full or traceable event/act contexts: • Accountability • Data Integrity • Clinical • Administrative/Operational



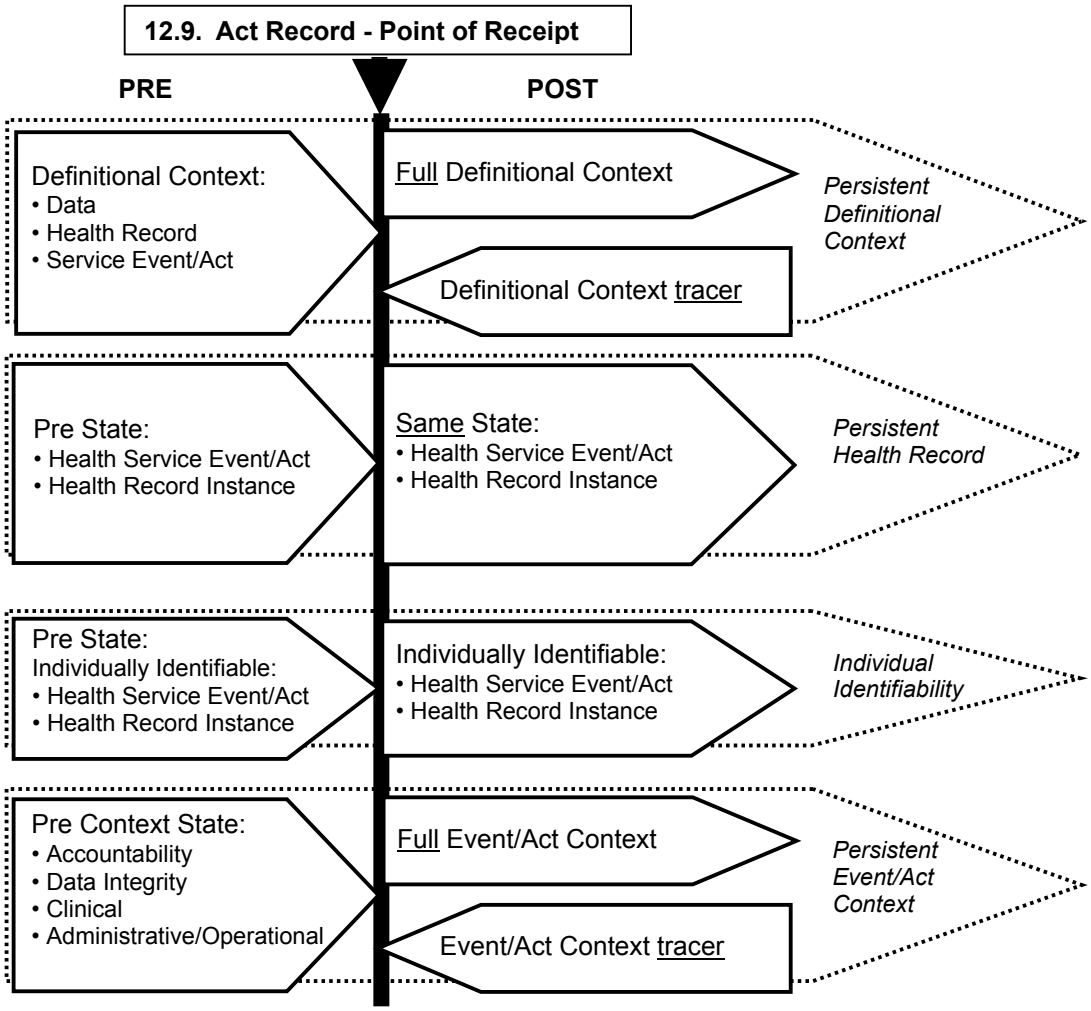
12.7. Act Record - Point of Convergence: **e.g., aggregation, summarization, derivation**	• Preserve health record instance pre-state. • Produce new record aggregations, summaries, derivations, as applicable. • May or may not carry forward individually identifiable information. Carry forward full or traceable health service event/act contexts: • Accountability • Data Integrity • Clinical • Administrative/Operational



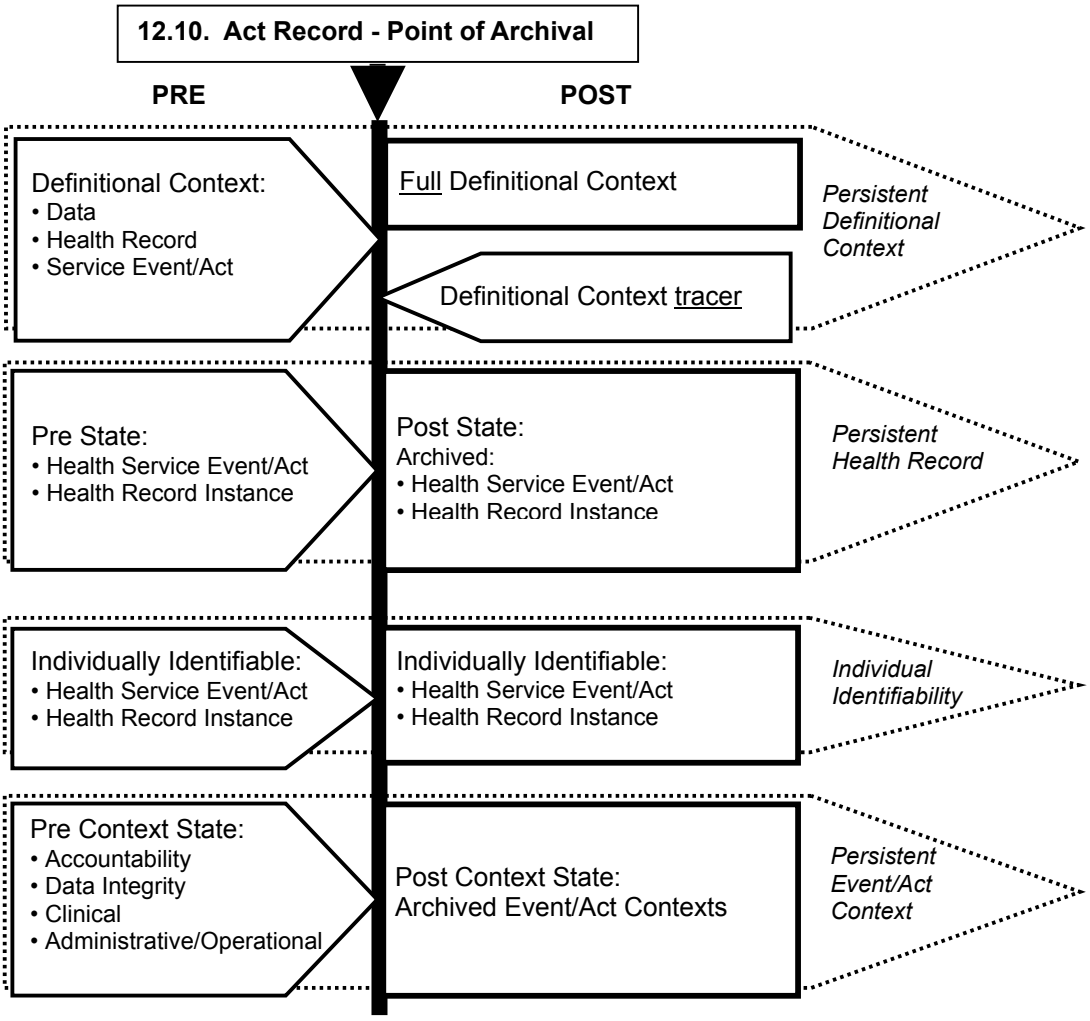
12.8.1. Act Record - Point of Disclosure, Transmittal **12.8.2. Act Record - Point of Reporting**	• Preserve health record instance pre-state • Append health record instance post-state as amendment **Accountability Context**, for this disclosure, transmittal or report: Record Instance ID Who - Record Subject - Individual Subject of Care ID Who – Steward/Transmitter (Disclosed By) - Accountable Healthcare Entity(ies), as pertains to each: <Digital Signature> Device, application or software ID Role, relative to record instance: steward Scope of accountability Who – Recipient (Disclosed To) - Accountable Healthcare Entity(ies), as pertains to each: <Digital Signature> Device, application or software ID Role, relative to record instance: steward Scope of accountability What - action: disclose, transmit, report When - date/time of disclosure, transmittal or reporting When – duration of valid use, as applicable Where - physical location Where - network address Why – purpose/intent of disclosure Carry forward full or traceable health service event/act context: • Accountability • Data Integrity • Clinical • Administrative/Operational



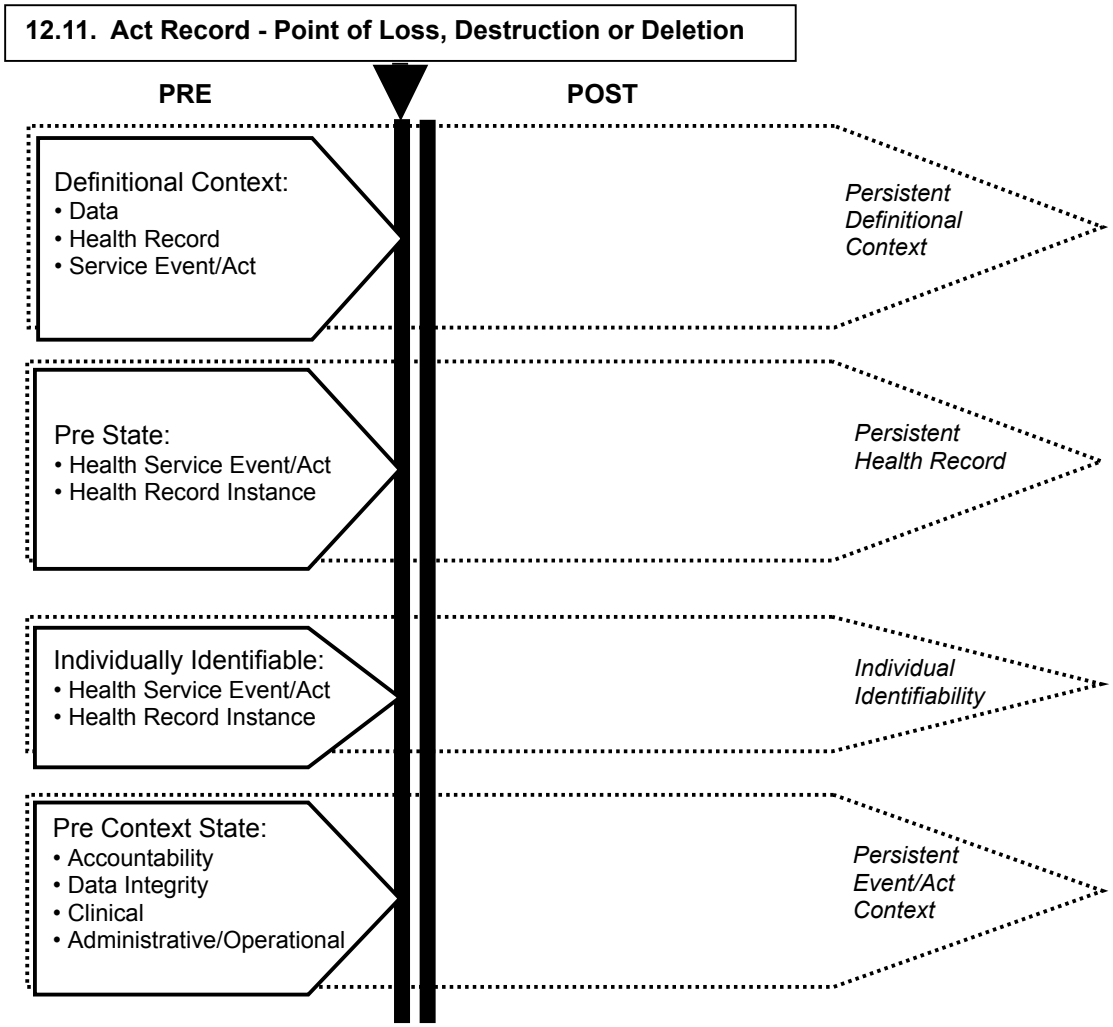
12.9. Act Record - Point of Receipt	• Preserve health record instance pre-state • Append health record instance post-state as amendment **Accountability Context**, for this receipt: Record Instance ID Who - Record Subject - Individual Subject of Care ID Who – Steward/Transmitter (Disclosed By) - Accountable Healthcare Entity(ies), as pertains to each: <Digital Signature> Device, application or software ID Role, relative to record instance: steward Scope of accountability Who – Recipient (Disclosed To) - Accountable Healthcare Entity(ies), as pertains to each: <Digital Signature> Device, application or software ID Role, relative to record instance: steward Scope of accountability What - action: receive When - date/time of receipt When – duration of valid use, as applicable Where - physical location Where - network address Why – purpose/intent of disclosure Carry forward full or traceable health service event/act context: • Accountability • Data Integrity • Clinical • Administrative/Operational



12.10. Act Record - Point of Archival	• Preserve health record instance pre-state • Archive health record instance



12.11. Act Record - Point of Loss, Destruction or Deletion	



Bibliography

[1] ISO/IEC TR 10000-1, Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework

[2] ISO/IEC Directives, Part 3, Rules for the structure and drafting of International Standards, 1997

[3] ISO 10241, International terminology standards — Preparation and layout

[4] ISO 31 (all parts), Quantities and units

[5] IEC 27 (all parts), Letter symbols to be used in electrical technology

[6] ISO 1000, SI units and recommendations for the use of their multiples and of certain other units

[7] ISO 690, Documentation — Bibliographic references — Content, form and structure

[8] Information Technology Security Evaluation Criteria. Published by the European Commission Version 1.3, 1992

[9] ISO/IEC 15414, Reference Model — Open Distributed Processing — Enterprise Viewpoint

[10] ISO/NIST, Common Criteria v2.0, ISO, US National Institute for Standards and Technology, 1999

[11] AHA, Toward a National Health Information Infrastructure: Report of the Work Group on Computerization of Patient Records (to the Secretary of the US Department of Health and Human Services, American Hospital Association, 1993

[12] ASTM E1384, Standard Guide for Description for Content and Structure of the Computer-Based Patient Record, ASTM Subcommittee E31.19, 1996

[13] ASTM E1762, Guide for Electronic Authentication of Health Care Information, ASTM Subcommittee E31.20, 1995

[14] ASTM E1769, Guide for Properties of Electronic Health Records and Record Systems, ASTM Subcommittee E31.12, 1995

[15] CEN ENV 1613:1995, Medical Informatics — Messages for Exchange of Laboratory Information

[16] CEN ENV 12265:1996, Medical Informatics — Electronic Health Record Architecture15

[17] CEN ENV 12443:1996, Medical Informatics — Healthcare information framework

[18] CEN ENV 13606:1999, Health Informatics — Electronic Healthcare Record Communication, all parts

[19] CEN ENV 13608-1:2000, Security for Healthcare Communication, all parts

[20] CEN CR 13694:1999, Safety and Security Related Software Quality Standards for Healthcare

[21] CIHI, Roadmap Initiative, Canadian Institute for Health Information, Statistics Canada, 1998

[22] CPRI, Guidelines for Managing Information Security Programs at Organizations Using Computer-Based Patient Record Systems, Computer-based Patient Record Institute, 1996

[23] CPRI, Description of the Computer-based Patient Record and Computer-based Patient Record Systems, Computer-based Patient Record Institute, 1995

[24] CPRI, Guidelines for Establishing Information Security Policies at Organizations Using Computer-based Patient Records, Computer-based Patient Record Institute, 1995

[25] CPRI, Guidelines for Information Security Education Programs at Organizations Using Computer-based Patient Records, Computer-based Patient Record Institute, 1995

[26] DHHS, Internet Security Policy, U.S. Department of Health and Human Services, Health Care Financing Administration, 1998

[27] DOD, Trusted System Criteria (The Orange Book), U.S. Department of Defense, 1985/1992

[28] DOD, Glossary of Computer Security Terms, U.S. Department of Defense, 1988

[29] DOD, Military Health System — Minimum Essential Security Requirements, U.S. Department of Defense, 1998

[30] DOD/VA/IHS, Government Computer-based Patient Record (GCPR) — Statement of Objectives, U.S. Departments of Defense and Veterans Affairs, Indian Health Service, 1998

[31] HL7, Health Level 7 Secure Transactions Special Interest Group, Health Level Seven, 1998

[32] HIPAA, Security and Electronic Signature Standards; Proposed Rule, US Department of Health and Human Services, Health Care Financing Administration, 1998

[33] HIPAA, Standards for Privacy of Individually Identifiable Health Information; Final Rule, US Department of Health and Human Services, Health Care Financing Administration, 2000

[34] IOM, The Computer-based Patient Record — An Essential Technology for Health Care, US Institute of Medicine, 1991/1997

[35] IOM, Health Data in the Information Age — Use, Disclosure and Privacy, US Institute of Medicine, 1994

[36] JCAHO, Accreditation Standards for Healthcare Organizations, Joint Commission for the Accreditation of Healthcare Organizations,1999

[37] MEDSEC, Draft Standard — High Level Security Policies for Health Care Establishments, European Commission, Directorate General III, Health Care Security and Privacy in the Information Society, 1998

[38] NEHRT, A Health Information Network for Australia, Australian National Electronic Health Records Taskforce, 2000

[39] NCQA, Health Plan Employer Data and Information Set v3.0 (HEDIS), National Committee for Quality Assurance, 1998-2000

[40] NCVHS, Core Health Data Elements, U.S. Department of Health and Human Services, National Council on Vital and Health Statistics, 1996

[41] NHS, Information for Health — An Information Strategy for the Modern NHS, U.K. National Health Service, 1998

[42] NRC, Computers at Risk — Safe Computing in the Information Age, US National Research Council, 1991

[43] OMG, Object Management Group Publications 1997, Chapter 15, Object Management Group, 1997

[44] OTA,, US Office of Technology Assessment, 1993

[45] U.S. Public Law 93-579: Federal Privacy Act of 1974

[46] U.S. Public Law 104-191: Health Insurance Portability and Accountability Act of 1996 (HIPAA)

[47] WEDI, Strategic National Implementation Plan (SNIP), Work Group for Electronic Data Interchange, 2000

[48] Digital Image Communication (DICOM). Version 3.0, ACR/NEMA

[49] ANSI/ADA 1000, Standard Clinical Data Architecture for the Structure and Content of an Electronic Health Record, American Dental Association, February 2001

ICS 35.240.80

Price based on 47 pages