TECHNICAL SPECIFICATION

ISO/TS 13606-4

First edition
2009-10-01

Health informatics — Electronic health record communication —

Part 4: Security

Informatique de santé — Communication du dossier de santé informatisé —

Partie 4: Sécurité

Reference number
ISO/TS 13606-4:2009(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 ... iv

0 Introduction ... v
0.1 Challenge addressed by this part of ISO 13606 ... v
0.2 Communication scenarios ... vii
0.3 Requirements and technical approach ... x
0.4 Generic EHR access policy model ... xiii
0.5 Audit log interoperability ... xviii
0.6 Relationship to ENV 13606-3 ... xix

1 Scope ... 1

2 Conformance ... 1

3 Terms and definitions ... 2

4 Abbreviations ... 4

5 Record component sensitivity and functional roles ... 4
5.1 RECORD_COMPONENT sensitivity ... 4
5.2 Functional roles ... 5
5.3 Mapping of functional role to RECORD_COMPONENT sensitivity ... 5

6 Representing access policy information within an EHR_EXTRACT ... 6
6.1 General ... 6
6.2 Archetype of the Access policy COMPOSITION ... 8
6.3 ADL representation of the archetype of the access policy COMPOSITION ... 10
6.4 UML representation of the archetype of the access policy COMPOSITION ... 15

7 Representation of audit log information —EHR_AUDIT_LOG_EXTRACT model ... 17

Annex A (informative) **Illustrative access control example** ... 19

Annex B (informative) **Relationship of this part of ISO 13606 to ENV 13606-3:2000** ... 23

Bibliography ... 29

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 other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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/TS 13606-4 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

ISO 13606 consists of the following parts, under the general title *Health informatics — Electronic health record communication*:

— *Part 1: Reference model*

— *Part 2: Archetype interchange specification*

— *Part 3: Reference archetypes and term lists*

— *Part 4: Security* [Technical Specification]

— *Part 5: Interface specification*

0 Introduction

0.1 Challenge addressed by this part of ISO 13606

The communication of electronic health records (EHRs) in whole or in part, within and across organizational boundaries, and sometimes across national borders, is challenging from a security perspective. Health records should be created, processed and managed in ways that guarantee the confidentiality of their contents and legitimate control by patients in how they are used. Around the globe these principles are progressively becoming enshrined in national data protection legislation. These instruments declare that the subject of care has the right to play a pivotal role in decisions on the content and distribution of his or her electronic health record, as well as rights to be informed of its contents. The communication of health record information to third parties should take place only with patient consent (which may be any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed). For EHR communication across national borders ISO 22857 provides guidance that may be used to define appropriate security policy specifications.

Ideally, each fine grained entry in a patient's record should only be accessed by those persons who have a right to view that information, specified by or approved by the patient and reflecting the dynamic nature of the set of persons with legitimate duty of care towards the patient through his or her lifetime. The access control list will ideally also include those persons who have a right to access the data for reasons other than a duty of care (such as health service management, epidemiology and public health, consented research) but exclude any information that they do not need to see or which the patient feels is too personal for them to access. On the opposite side, the labelling by patients or their representatives of information as personal or private should ideally not hamper those who legitimately need to see the information in an emergency, nor accidentally result in genuine healthcare providers having such a filtered perspective that they are misled into managing the patient inappropriately. Patients' views on the inherent sensitivity[1] of entries in their health record may evolve over time, as their personal health anxieties alter or as societal attitudes to health problems change. Patients might wish to offer some heterogeneous levels of access to family, friends, carers and members of their community. Families may wish to provide a means by which they are able to access parts of each other's records (but not necessarily to equal extents) in order to monitor the progress of inherited conditions within a family tree.

Such a set of requirements is arguably more extensive than that required of the data controllers in most other industry sectors. It is in practice made extremely complex by:

- numbers of health record entries made on a patient during the course of modern healthcare;
- numbers of healthcare personnel, often rotating through posts, who might potentially come into contact with a patient at any one time;
- numbers of organizations with which a patient might come into contact during his or her lifetime;
- difficulty (for a patient or for anyone else) of classifying, in a standardized way, how sensitive a record entry might be;
- difficulty of determining how important a single health record entry might be to the future care of a patient and to which classes of user;

1) The term “sensitivity” is widely used in the security domain for a broad range of safeguards and controls, but in this part of ISO 13606 the term refers only to access controls.

— logically indelible nature of the EHR and the need for revisions to access permissions to be rigorously managed in the same way as revisions to the EHR entries themselves;

— need to determine appropriate access very rapidly, in real time, and potentially in a distributed computing environment;

— high level of concern expressed by a growing minority of patients to have their consent for disclosure recorded and respected;

— low level of concern the majority of patients have about these requirements, which has historically limited the priority and investment committed to tackling this aspect of EHR communications.

To support interoperable EHRs, and seamless communication of EHR data between healthcare providers, the negotiation required to determine if a given requester for EHR data should be permitted to receive the data needs to be capable of automation. If this were not possible, the delays and workload of managing human decisions for all or most record communications would obviate any value in striving for data interoperability.

The main principles of the approach to standards development in the area of EHR communications access control are to match the characteristics and parameters of a request to the EHR provider's policies, and to any access control or consent declarations within the specified EHR, to maintain appropriate evidence of the disclosure, and to make this capable of automated processing.

In practice, efforts are in progress to develop International Standards for defining access control and privilege management systems that would be capable of computer-to-computer negotiation. However, this kind of work is predicated upon health services agreeing a mutually consistent framework for defining the privileges they wish to assign to staff, and the spectrum of sensitivity they offer for patients to define within their EHRs.

This requires consistency in the way the relevant information is expressed, to make this sensibly scalable at definition-time (when new EHR entries are being added), at run-time (when a whole EHR is being retrieved or queried) and durable over a patient's lifetime. It is also important to recognise that, for the foreseeable future, diversity will continue to exist between countries on the specific approaches to securing EHR communications, including differing legislation, and that a highly prescriptive approach to standardization is not currently possible.

This part of ISO 13606 therefore does not prescribe the access rules themselves (i.e. it does not specify who should have access to what and by means of which security mechanisms); these need to be determined by user communities, national guidelines and legislation. However it does define a basic framework that can be used as a minimum specification of EHR access policy, and a richer generic representation for the communication of more fine-grained detailed policy information. This framework complements the overall architecture defined in ISO 13606-1, and defines specific information structures that are to be communicated as part of an EHR_EXTRACT defined in ISO 13606-1.

The formalisms used to represent policy specifications in this part of ISO 13606 include Unified Modelling Language (UML: please see http://www.omg.org/technology/documents/formal/uml.htm for more information) and Archetype Definition Language (ADL: please see http://www.openehr.org/120-OE.html for more information).

Some of the kinds of agreement necessary for the security of EHR communication are inevitably outside the scope of this part of ISO 13606. The complete protection of EHR communication requires attention to a large number of issues, many of which are not specific to health information.

NOTE This document is based on EN 13606-4:2007. The content of this part of ISO 13606 is identical to that of EN 13606-4 with the following exceptions:

— the wording of this Introduction has been revised to reflect its international rather than European jurisdiction;

— references to a security standard in development have been updated if that standard has now been published;

— relationships to new security standards in development have been added where appropriate;

— the first entry in Table 2 (sensitivity level classification) has been changed from “personal care” to “personal”;

— a small number of typographic errors and ambiguous expressions within this introduction have been corrected.

0.2 Communication scenarios

0.2.1 Data flows

The interfaces and message models required to support EHR communication are the subject of ISO 13606-5. The description here is an overview of the communications process in order to show the interactions for which security features are needed. Figure 1 illustrates the key data flows and scenarios that need to be considered by this part of ISO 13606. For each key data flow there will be an acknowledgement response, and optionally a rejection may be returned instead of the requested data.

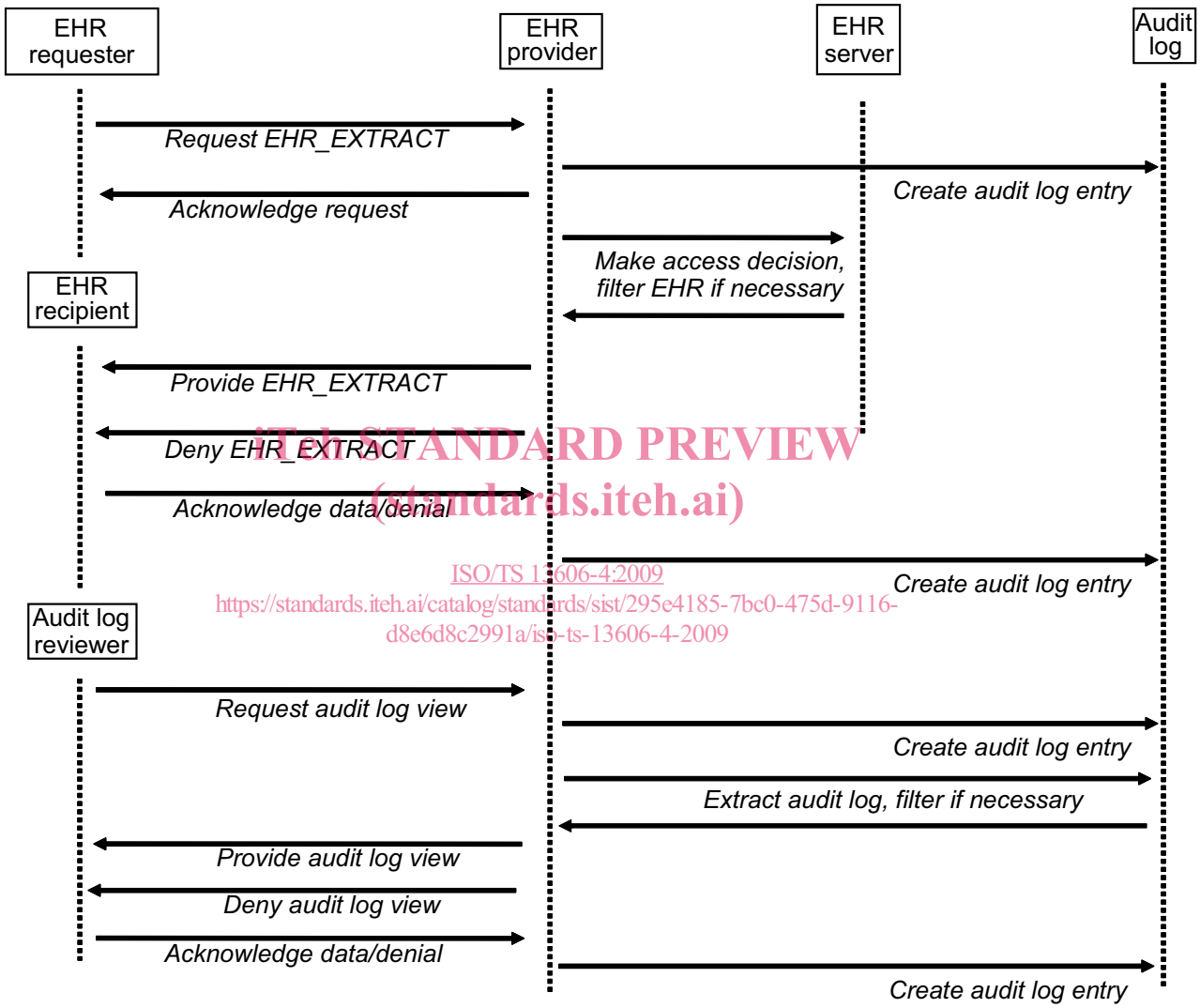

Figure 1 — Principal data flows and security-related business processes covered by this part of ISO 13606

The EHR requester, EHR recipient and audit log reviewer might be healthcare professionals, the patient, a legal representative or another party with sufficient authorization to access healthcare information. Both the EHR_EXTRACT and the audit log, if provided, may need to be filtered to limit the disclosure to match the privileges of the recipient. This aspect of access control is discussed later in this Introduction.

NOTE all parties shown here will need to maintain an audit log, not just the EHR provider. However, for readability the other audit log processes are not shown or described here.

0.2.2 Request EHR data

This interaction is not always required (for example, EHR data might be pushed from provider to recipient as in the case of a discharge summary). The request interface needs to include a sufficient profile of the requester to enable the EHR provider to be in a position to make an access decision, to populate an audit log, and provide the appropriate data to the intended recipient. In some cases the EHR requester might not be the same party as the EHR recipient – for example a software agent might trigger a notification containing EHR data to be sent to a healthcare professional. In such cases it is the EHR recipient's credentials that will principally determine the access decision to be made.

An EHR request may need to include or reference consents for access and mandates for care, e.g. by providing some form of explicit consent from the patient, or a care mandate.

The negotiation between requester and provider of EHR data will increasingly be automated, and the information included in this interaction is required to be sufficient to enable a fully computerized policy negotiation.

The requirements for this interaction will be reflected in the EHR_Request interface model defined in ISO 13606-5.

0.2.3 Generate EHR access log entry

This is assumed practice in any EHR system, but it is not specified as a normative interface because of the diverse approaches and capabilities in present-day systems. The internal audit systems within any EHR system are not required to be interoperable except in support of the model defined in Clause 7 and the corresponding interface defined in ISO 13606-5.

0.2.4 Acknowledge receipt of EHR_Request

No healthcare-specific security considerations.

0.2.5 Make access decision, filter EHR data

When processing the EHR request, policies pertaining to the EHR provider and access policies in the EHR itself all need to be taken into account in determining what data are extracted from the target EHR. This part of ISO 13606 cannot dictate the overall set of policies that might influence the EHR provider, potentially deriving from national, regional, organization-specific, professional and other legislation.

A decision to filter the EHR data on the basis of its sensitivity and the privileges of the EHR requester and recipient will need to conform to relevant policies and may need to balance the clinical risks of denying access to information with the medico-legal risks of releasing information.

This part of ISO 13606 however does define an overall framework for representing, in an interoperable way, the access policies that might relate to any particular EHR, authored by the patient or representatives. These might not be stored in the physical EHR system in this way; they might instead, for example, be integrated within a policy server linked to the EHR server.

This access decision is discussed in more detail in Clause 5.

0.2.6 Deny EHR_EXTRACT

If the access decision is to decline, a coarse-grained set of reasons needs to be defined in order to frame a suitable set of responses from the EHR provider. However, it is important that the denial and any reason given does not imply to the recipient that the requested EHR data does exist – even the disclosure of its existence could itself be damaging to a patient.

No healthcare-specific security considerations; the interface model is defined in ISO 13606-5.

0.2.7 Provide EHR_EXTRACT

Note that the EHR recipient need not be the same as an EHR requester, and indeed the provision of an EHR need not have been triggered by a request. It might instead have been initiated by the provider as part of a shared care pathway or to add new data to an existing EHR.

The EHR_EXTRACT is required to conform to the reference model defined in ISO 13606-1, and to the interface model defined in ISO 13606-5.

The EHR_EXTRACT is required to include or to reference any relevant access policies, represented in conformance with this part of ISO 13606, to govern any onward propagation of the EHR data being communicated. Policies may only be referenced if the EHR recipient is known to have direct access to the same information by another means.

0.2.8 Acknowledge receipt of EHR_EXTRACT

No healthcare-specific security considerations.

0.2.9 Generate EHR access log entry

(As 0.2.3)

0.2.10 Request EHR access log view

This is now considered to be desirable practice, to enable a patient to discover who has accessed part or all of his/her EHR in a distributed computing environment. The scope of this interface, as defined in this part of ISO 13606, is to request a view of the audit log that informs the recipient about who has accessed what parts of a given EHR and when. This interface is not intended to support situations where a full inspection of an audit log is required for legal purposes or for other investigations. This interface is discussed in Clause 5.

The interface model is defined in ISO 13606-5.

0.2.11 Generate EHR access log entry

(As 0.2.3)

0.2.12 Provide EHR access log view

This is desirable practice, and requires an interoperable representation of such an entry (or set of entries). This interface is discussed in Clause 5.

Although a legal investigation will require that an audit log is provided in a complete and unmodified form, the presentation of an audit log view to a patient or to a healthcare professional might require that some entries are filtered out (e.g. those referring to EHR data to which the patient does not have access).

The interface model is defined in ISO 13606-5.

0.2.13 Deny EHR access log view

If the request is not to be met, a coarse-grained set of reasons needs to be defined. However, it is important that the denial and any reason given does not imply to the recipient that the requested EHR data does exist – even the disclosure of its existence could itself be damaging to a patient.

No healthcare-specific security considerations; the interface model is defined in ISO 13606-5.

0.2.14 Acknowledge receipt of EHR access log view

No healthcare-specific security considerations.

0.2.15 Generate EHR access log entry

(As 0.2.3)

0.3 Requirements and technical approach

0.3.1 Research on the requirements

The vision of research, industry and previous standards on interoperable electronic health record communication has been to enable diverse clinical systems to exchange whole or parts of a patent's EHR in a standardized way that can rigorously and generically represent the data values, contextual organization and medico-legal provenance of the information in any originating EHR system. Sensitive information, such as that in EHR systems, has to be recorded, stored, processed and communicated in a secure, safe, and trustworthy way. EHR communication has therefore also to meet security requirements such as:

— authentication of entities (people, software, devices etc.) that might legitimately require or provide EHR data;

— authorization, privilege and access control management;

— integrity of the EHR information that is stored, processed and communicated;

— security classification of EHR information;

— definition, negotiation and bridging of policies between the entities requiring and providing EHR data;

— auditability and traceability of information accessed, processed and communicated;

— overall safety and quality procedures.

The research and development (R&D) background work in these fields includes European projects such as SEISMED, TrustHealth and HARP.

Most healthcare organization information systems already have security systems and services in place to protect a wide range of health related data flows, of which EHR communications is only one example. Furthermore, the field of health informatics security is actively developing generic approaches to specifying, implementing, profiling and evaluating ever-enhanced security services. Many of the requirements that pertain to EHR communications are therefore also applicable to healthcare communications in general.

0.3.2 Generic healthcare security requirements

The most widely accepted requirements for an overall security approach in domains handling sensitive and personal data are published in ISO/IEC 27002. This specifies the kinds of measure that should be taken to protect assets such as EHR data, and ways in which such data might safely be communicated as part of a distributed computing environment. A health specific guide to this general standard has been published in ISO 27799. This will facilitate the formulation of common security policies across healthcare, and should help promote the adoption of interoperable security components and services.

For EHR communication across national borders ISO 22857 provides guidance that may be used to define appropriate security policy specifications.

The exact security requirements that are required to be met to permit any particular EHR communication instance will be governed by a number of national and local policies at both the sending and receiving sites, and at any intermediate links in the communications chain. Many of these policies will apply to healthcare communications in general, and will vary between countries and clinical settings in ways that cannot and should not be directed by this part of ISO 13606.

For example, any access to EHR data will require that the requesting party is appropriately authenticated, that he, she or it is authorized to make the request and that, if met, the nominated recipient of EHR data (who might not always be the requester) is authorized to receive it. All communications are required to take place through secured communications channels, and an audit log is required to be kept of all EHR data flows. The infrastructure to provide for these security services will be generic to many secure domains, not just for healthcare, and this part of ISO 13606 assumes that these services will be in place and used for every EHR communication.

The approach taken in drafting this part of ISO 13606 has therefore been to assume that generic security policies, components and services will contribute to a negotiation phase (the *access decision*) prior to sanctioning the communication of an EHR extract and will protect the actual EHR data flows.

This part of ISO 13606 therefore assumes that an overall security policy or set of policies conforming to ISO 27799 is in place at all of the sites participating in an EHR communication, and also that these policies conform to national or trans-border data protection legislation. Additional policies may be required to conform to specific national, local, professional or organization regulations applicable to the communication or use of EHR data. Defining such policies is beyond the scope of this part of ISO 13606.

0.3.3 Generic healthcare access control architecture

Legitimate access to EHR data will be determined by a wide range of policies, some of which might exist as documents, some will be encoded within applications and some within formal authorization system components. It is recognised that vendors and organizations differ in how they have implemented access control policies and services and the extent to which these are currently computerized.

ISO/TS 22600 defines a generic logical model for the representation of the privileges of principals (entities), of access control policies that pertain to potential target objects, and of the negotiation process that is required to arrive at an access decision. This part of ISO 13606 specifies a generic approach to tasks such as the assignment of roles to entities and the passing of roles between entities.

Figure 2 depicts the key concepts of role based access control, as defined by ISO/TS 22600.

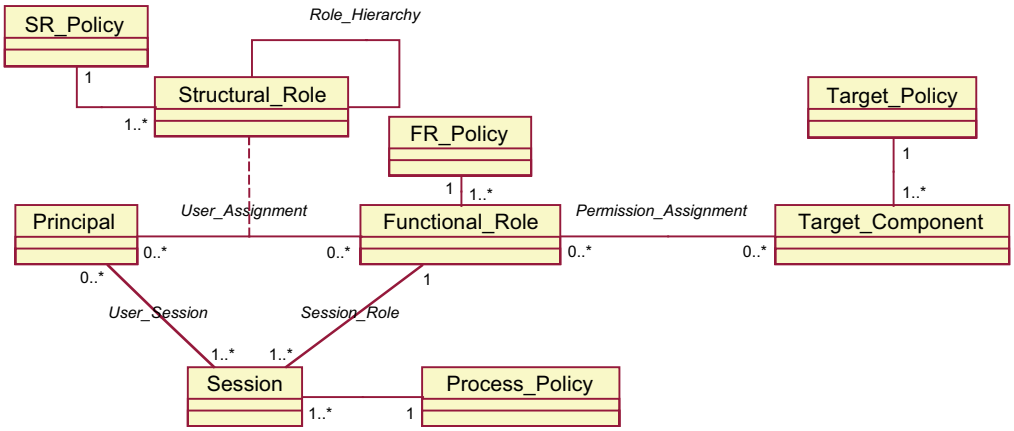

Figure 2 — Main concepts and policy types defined in role based access control

Principals (persons, agents etc.) are mapped to one or more functional roles, which will be influenced by the structural roles that they are permitted to hold. For example, a person who is medically qualified and a specialist in child health may hold one or more structural roles (such as consultant paediatrician at a hospital, head of child screening for the region). Those structural roles may permit him or her at times to act with the functional role of personal clinician to a patient. The functional role might be persistent, or limited to a single user session. Functional roles are mapped to permissions to perform particular operations (such as writing new entries in an EHR) and to particular objects (e.g. the EHR data which that role-holder is permitted to view).

For the purposes of this part of ISO 13606, the Target_Component class shown in Figure 2 is the EHR data held by the EHR provider. The Target_Policy class contains information that defines rules to permit or deny access to part or all of the EHR. If an EHR_EXTRACT is created and communicated with these EHR data, the pertinent Target_Policies need also to be communicated to the EHR recipient. This requires an interoperable representation of a Target_Policy that can be included within an EHR_EXTRACT.

Because individual vendors and organizations may differ in their engineering and technology implementations to achieve this infrastructure, ISO/TS 22600 defines these processes and models at the information and computational viewpoint levels. Its specifications are therefore open, platform-independent, portable and scalable to support a wide range of clinical settings and use in different countries where national and professional regulations may be different.

This part of ISO 13606 assumes that the ISO/TS 22600 approach is logically applied to govern access decisions in response to an EHR request. However, it is not in its scope to define the actual policy models, attributes or attribute values that are needed to represent individual policy instances, or the way in which the ISO/TS 22600 logical approach is technically implemented in any organization or region.

As a complement to that emerging standard, ISO/TS 21298 defines sets of structural roles and functional roles that can be used internationally to support policy negotiation and policy bridging (e.g. during the negotiation phase of an access decision). This part of ISO 13606 recognises that these and other standardized vocabularies will increasingly support rich interoperability of access policies, but cannot mandate the use of any particular controlled vocabulary since none exists as a formal standard.

0.3.4 Security requirements specific to EHR communications

A large number of EHR-specific medico-legal and ethical requirements are expressed within ISO/TS 18308, although compliance with these is primarily met through specific classes and attributes of the EHR reference model (published in ISO 13606-1). Table 1 lists those requirements that apply most specifically to this part of ISO 13606.

Table 1 — List of requirements published in ISO/TS 18308 that relate to the security of EHR communications

COC1.2	EHRA shall support consumers' right of access to all EHR information subject to jurisdictional constraints.
COC1.3	EHRA shall support consumers' being able to incorporate self-care information, their point of view on personal healthcare issues, levels of satisfaction, expectations and comments they wish to record in EHRs.
COM2.4	EHRA shall provide an audit trail of exchange processes, including authentication, to enable identification of points of EHR extract transmittal and receipt. This needs to account for merging processes.
PRS1.2	EHRA shall support the labelling of the whole and/or sections of the EHR as restricted to authorized users and/or purposes. This should include restrictions at the level of reading, writing, amendment, verification and transmission/disclosure of data and records.
PRS1.3	EHRA shall support privacy and confidentiality restrictions at the level of both data sets and discrete data attributes.
PRS2.2	EHRA shall support obtaining, recording and tracking the status of informed consent[2)] to access the whole and/or sections of the EHR, for defined purposes.
PRS2.4	EHRA shall support recording of the time frames attached to each consent.
PRS3.1	EHRA shall support measures to define, attach, modify and remove access rights to the whole and/or sections of the EHR.
PRS3.3	EHRA shall support measures to enable and restrict access to the whole and/or sections of the EHR in accordance with prevailing consent and access rules.
PRS3.4	EHRA shall support measures to separately control authorities to add to and/or modify the EHR from authorities to access the EHR.
PRS5.1	EHRA shall support recording of an audit trail of access to and modifications of data within the whole or sections of the EHR.
PRS5.2	EHRA shall support recording of the nature of each access and/or modification.
STR2.10	EHRA shall allow for comprehensive information storage and retrieval regarding patient care. The EHRA shall at a minimum allow for the recording of all structured and unstructured data on: others; disclosures and consent.

0.4 Generic EHR access policy model

0.4.1 Factors considered when defining EHR access policies

In addressing these requirements within this part of ISO 13606, it is recognised that most clinical and EHR systems deployed today incorporate relatively simple access control measures, usually to support needs within a single organization. Few of these are interoperable across vendor products or with other relevant systems such as decision support, workflow or reporting systems. New-generation systems will increasingly permit configurable access policies to be specified, but in order to support a distributed EHR scenario these will need to be interoperably specified and interoperable computationally. Most vendors, health services and healthcare networks are likely to adopt an incremental approach to enriching the sophistication of access control policies that can be supported.

There might be a range of high-level policies that will govern EHR disclosures within any regional healthcare network. Today these will exist primarily on paper or as hard-coded permissions within applications and servers, but in future these will be represented as interoperable access policies in accordance with the ISO/TS 22600 architecture. Some example factors that might be specified within such policies, and taken into account when making an EHR access decision, are listed below.

2) It is now recognised that implied or inferred consent also needs to be supported.

National, professional and organizational policies might be based upon, for example:

User characteristics:

- name and identification;
- profession, speciality, qualifications;
- functional role;
- department or clinical speciality of which he/she is acting as a member;
- organization of which he/she is acting as a member.

Access characteristics:

- date and time;
- location;
- physical device;
- network or other communications mechanism;
- mechanisms and extent of encryption in place;
- method of authentication used.

Organizational policies might also confirm permissions about:

- the patient whose record is being accessed;
- the archetypes being accessed;
- the operation proposed (read, write, modify, communicate, query etc.).

EHR-specific policies might provide or deny consent for:

a) named/identified parties

- to access the EHR as a whole;
- to adopt particular functional or structural roles (e.g. to specify a responsible personal healthcare agent);

b) specific clinical settings (e.g. departments, specialities);

c) specific functional roles;

- to access particular archetypes;
- to access particular record components ;
- to access data of specific sensitivity;
- to undertake specific EHR functions (e.g. read, write, modify, communicate, query);

d) specific purposes for the access;

— e.g. direct care provision, support of care provision, teaching, research;

— justification or evidence required (e.g. if a formal signed consent is required to be provided).

The whole spectrum of access policies in place at an organization is beyond the scope of this part of ISO 13606, but it does define a generic specification for representing and communicating those parts of access policies that relate directly to the data within any given EHR (target policies). These will often be representations of the disclosure wishes of the patient.

The communication of the specific consents and access policies expressing the wishes of patients or their representatives is an important aspect of EHR communication and interoperability. Such policies will contribute to the overall access decision made in response to EHR requests, and need to be transferred along with the extracted EHR data to the EHR recipient, in order for the recipient to apply these policies to govern any future accesses to the same data from their organization.

A generic model to represent consent/access policies expressing the wishes of the patient or other parties is therefore defined in this part of ISO 13606, in Clause 6. Those EHR-specific policies that need to be included within an EHR_EXTRACT may be represented using the model specified in Clause 6. This model is deliberately extensible to handle additional policy specifications not foreseen at the time of producing this part of ISO 13606. Because ISO/TS 22600-3 is expected to define an interoperable access policy model that can be used for this purpose, a UML model is also defined in Clause 6 to permit adopters of this part of ISO 13606 to conform both to this and to ISO/TS 22600.

In ISO 13606-1 reference model every RECORD_COMPONENT within the EHR_EXTRACT includes an optional Policy_ID attribute to permit references to such policies to be made at any level of granularity within the EHR containment hierarchy. Every RECORD_COMPONENT can therefore reference any number of access policies or consent declarations that define the intended necessary privileges and profiles of principals (users, agents, software, devices, delegated actors etc.) for future access to it.

Note that some policies may apply to particular RECORD_COMPONENTs within an EHR, whilst others may apply to the EHR as a whole.

0.4.2 EHR access policies: a minimum specification for interoperability

0.4.2.1 General

The information model in Clause 6, for representing and communicating access policy information, has been deliberately kept very generic, to allow for the diversity of policy criteria that will be stipulated in different countries and regional healthcare networks. Standardized vocabularies for many of the likely characteristics are not currently defined. The policy model in Clause 6 is therefore only a partial aid to policy interoperability.

A number of existing and legacy systems might not be able to incorporate richly-defined policy specifications, and many healthcare regions might not be in a position to define such policies for some years. Therefore, as a complement to the overall policy model in Clause 6, this part of ISO 13606 defines two vocabularies that can provide a minimum basis for making an access policy decision, and ensure a basic level access policy interoperability, albeit at a coarse-grained level.

These two vocabularies are:

1) sensitivity classification of EHR data (RECORD_COMPONENTS);

2) high-level classification of EHR requesters and recipients, through a set of functional roles.