

DIN EN ISO 13606-4

ICS 35.240.80

Einsprüche bis 2017-07-05
Vorgesehen als Ersatz für
DIN EN 13606-4:2007-06

Entwurf

**Medizinische Informatik –
Kommunikation von Patientendaten in elektronischer Form –
Teil 4: Sicherheit (ISO/DIS 13606-4:2017);
Englische Fassung prEN ISO 13606-4:2017**

Health informatics –
Electronic health record communication –
Part 4: Security (ISO/DIS 13606-4:2017);
English version prEN ISO 13606-4:2017

Informatique de santé –
Communication du dossier de santé informatisé –
Partie 4: Sécurité (ISO/DIS 13606-4:2017);
Version anglaise prEN ISO 13606-4:2017

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2017-05-05 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an named@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Medizin (NAMED), 10772 Berlin, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 49 Seiten

DIN-Normenausschuss Medizin (NAMED)

Nationales Vorwort

Dieses Dokument (prEN ISO 13606-4:2017) wurde in der WG 1 „Architecture, Frameworks and Models“ des Technischen Komitees ISO/TC 215 „Health Informatics“ und mit dem Technischen Komitee CEN/TC 251 „Medizinische Informatik“, dessen Sekretariat von NEN (Niederlande) gehalten wird, erarbeitet. Der Arbeitsausschuss NA 063-07-02 AA „Interoperabilität“ des Fachbereichs 7 „Medizinische Informatik“ des DIN-Normenausschusses Medizin (NAMed) hat an der Erarbeitung ebenfalls mitgewirkt.

Dieses Dokument enthält unter Berücksichtigung des Präsidialbeschlusses 1/2004 nur die englische Originalfassung von prEN ISO 13606-4:2017.

Änderungen

Gegenüber DIN EN 13606-4:2007-06 wurden folgende Änderungen vorgenommen:

- a) Übernahme der Internationalen Norm;
- b) der Norminhalt wurde mit ISO 13940 *Medizinische Informatik — Begriffssystem zur Unterstützung der Kontinuität der Versorgung* und der Normenreihe ISO 12967 *Medizinische Informatik — Servicearchitektur* und harmonisierte;
- c) die Teile dieser Normenreihe wurden untereinander harmonisiert.

Zusammenfassung

Dieser Teil dieser mehrteiligen Norm zur eGA-Übermittlung beschreibt eine Methodik zur Spezifikation der Privilegien, die für den Zugriff auf eGA-Daten erforderlich sind. Diese Methodik ist Teil der gesamten eGA-Übermittlungsarchitektur, die in ISO 13606 Teil 1 definiert ist.

Dieser Teil von ISO 13606 verfolgt die Absicht, die Anforderungen, die sich ausschließlich auf die eGA-Übermittlung beziehen, zu behandeln und eGA-spezifische Informationen darzustellen und zu übermitteln, die eine Zugangsentscheidung unterstützen. Er bezieht sich auch auf allgemeine Sicherheitsanforderungen, die für die eGA-Übermittlung gelten, und zeigt technische Lösungen und Normen auf, welche Einzelheiten zu Diensten spezifizieren, die diese Sicherheitsanforderungen erfüllen.

ANMERKUNG Sicherheitsanforderungen für eGA-Systeme, die nicht mit der Übermittlung von eGAs zusammenhängen, liegen außerhalb des Anwendungsbereichs dieses Teils von ISO 13606.

Nationaler Anhang NA (informativ)

Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach EN ISO 13606-1 und die folgenden Begriffe.

3.1

Attributautorisierer

(AA, en: attribute authority)

Behörde, die durch Ausgabe von Attributzettifikaten Privilegien zuweist

[ISO/IEC 9594-8:1995]

3.2

Autorisierer

(en: authority)

Entität, die für die Ausgabe von Zertifikaten verantwortlich ist

Anmerkung 1 zum Begriff: In dieser Spezifikation werden zwei Typen unterschieden: Zertifizierungsstelle, die Public-Key-Zertifikate ausstellt und Attributautorisierer, der Attributzettifikate ausstellt

3.3

Verfügbarkeit

(en: availability)

Eigenschaft, einer berechtigten Instanz auf Verlangen zugänglich und nutzbar zu sein

[QUELLE: ISO 7498-2:1989]

3.4

Zertifizierungsstelle

(CA, en: certification authority)

Behörde, die von einer oder mehreren vertrauenden Parteien als vertrauenswürdig erachtet wird, um Zertifikate erstellen, zuweisen und verwalten zu können

Anmerkung 1 zum Begriff: Wahlweise kann die Zertifizierungsstelle die Schlüssel der vertrauenden Parteien erzeugen [ISO 9594-8:1995]. Die CA gibt Zertifikate durch Signieren von Zertifikatsdaten mit ihrem privaten Signaturschlüssel aus.

Anmerkung 2 zum Begriff: Die Bezeichnung der CA als Behörde meint in diesem Zusammenhang keine Regierungsbehörde, sondern nur, dass die betreffende Einrichtung als vertrauenswürdig erachtet wird. Zertifikatsaussteller ist möglicherweise die bessere Benennung, Zertifizierungsstelle (CA) ist aber wesentlich gebräuchlicher.

3.5

Identifikator

(en: identifier)

Information, die verwendet wird, um vor einer möglichen Bestätigung durch einen entsprechenden Authentifikator eine Identität zu beanspruchen

3.6

Policy

(en: policy)

Satz von rechtlichen, politischen, organisationsinternen, funktionellen und technischen Pflichten im Hinblick auf Kommunikation und Kooperation [ISO 22600:2014]

3.7

Privileg

(en: privilege)

Fähigkeit, die einer Entität von einer Autorität zugewiesen wird [ISO 22600:2014]

3.8

Sensibilität

(en: sensitivity)

Eigenschaft einer Ressource, die deren Wert oder Wichtigkeit impliziert [ISO 22600:2014]

Contents

Foreword	5
0 Introduction (Informative)	6
0.1 General	6
0.2 Challenge addressed by this part of EN ISO 13606	6
0.3 Communication scenarios	8
0.4 Requirements and technical approach	12
0.5 EHR access policy model	14
0.6 Audit log interoperability	18
1 Scope	19
2 Normative references	19
3 Terms and definitions	19
4 Abbreviations	21
5 Conformance	22
6 Record Component Sensitivity and Functional Roles	23
6.1 RECORD_COMPONENT sensitivity	23
6.2 Functional roles	23
6.3 Mapping of Functional Role to COMPOSITION sensitivity	24
7 Representing access policy information within an EHR_EXTRACT	25
7.1 Overview	25
7.2 UML representation of the archetype of the access policy COMPOSITION	27
7.3 Archetype of the access policy COMPOSITION	33
8 Representing audit log information	34
Annex A - Illustrative access control example	41
Annex B - Relations of ISO 13606-4 to alternative approaches	45

- Entwurf -

Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2. www.iso.org/directives

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received. www.iso.org/patents

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 215.

0 Introduction (Informative)

0.1 General

This Standard, EN ISO 13606 Part 4, is part of a five-part standard series, published jointly by CEN and ISO through the Vienna Agreement. These five parts are as follows.

Part 1: Reference Model. An information model, represented in UML, that may be used to communicate the content and context of any possible electronic health record information, for part or all of a person's electronic health record, or potentially for a set of persons such as a family. This model supports communication between distinct electronic health record repositories or may act as the information model underpinning a federation, such as a regional, national or multi-national network of interconnected repositories of EHR data.

Part 2: Archetype Interchange Specification. An information model represented in UML, accompanied by requirements, for the representation of clinical models which specify how individual areas of clinical information should be represented using the reference model of part 1.

Part 3: Reference Archetypes and Term Lists. A set of high-level archetype patterns that may be used (specialised) to develop specific archetypes covering commonly needed areas of clinical and demographic information. This part standard also includes a set of vocabularies (term lists) to populate properties of the information models included in other parts of this overall standard.

Part 4: Security. A vocabulary framework, and a more detailed generic representation for policy information, to communicate the access permissions covering the EHR content that is being communicated according to this standard. This part standard additionally contains an interoperable specification for audit log information that could inform a subject of care about who has accessed their health record.

Part 5: Interchange Specification. The information properties that should be included within interfaces that implement communication according to the other parts of this standard.

In this part standard, dependency upon any of the other parts of this series is explicitly stated where it applies.

0.2 Challenge addressed by this part of EN ISO 13606

The communication of electronic health records (EHRs) in whole or in part, within and across organisational boundaries, and sometimes across national borders, is challenging from a security perspective. Health records should be created, processed and managed in ways that assure 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). More details can be found in ISO 22600-3. 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 permissions 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 permissions 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 health care providers having such a filtered perspective that they are misled into managing the patient inappropriately. Patients' views on the inherent sensitivity¹ 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:

- the large number of health record entries made on a patient during the course of modern health care;
- the large number of health care personnel, often rotating through posts, who might potentially come into contact with a patient at any one time;
- the large number of organizations with which a patient might come into contact during his or her lifetime;
- the difficulty (for a patient or for anyone else) of classifying in a standardized way how sensitive a record entry might be;
- the 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;
- the 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;
- the need to determine appropriate access very rapidly, in real time, and potentially in a distributed computing environment;
- the high level of concern expressed by a growing minority of patients to have their consent for disclosure recorded and respected;
- the 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 health care providers, the negotiation required to determine if a given requester for EHR data should be permitted

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.

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 recognize 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 presently 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 EN ISO 13606 Part 1, and defines specific information structures that are to be communicated as part of an EHR_EXTRACT defined in Part 1. Some of the kinds of agreement necessary for the security of EHR communication are inevitably outside the scope of this part of EN ISO 13606, and are covered more extensively in ISO 22600 (Privilege Management and Access Control).

0.3 Communication scenarios

0.3.1 Data flows

The interfaces and message models required to support EHR communication are the subject of EN ISO 13606 Part 5. The description here is an overview of the communications process in order to show the interactions for which security features are needed. The 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.

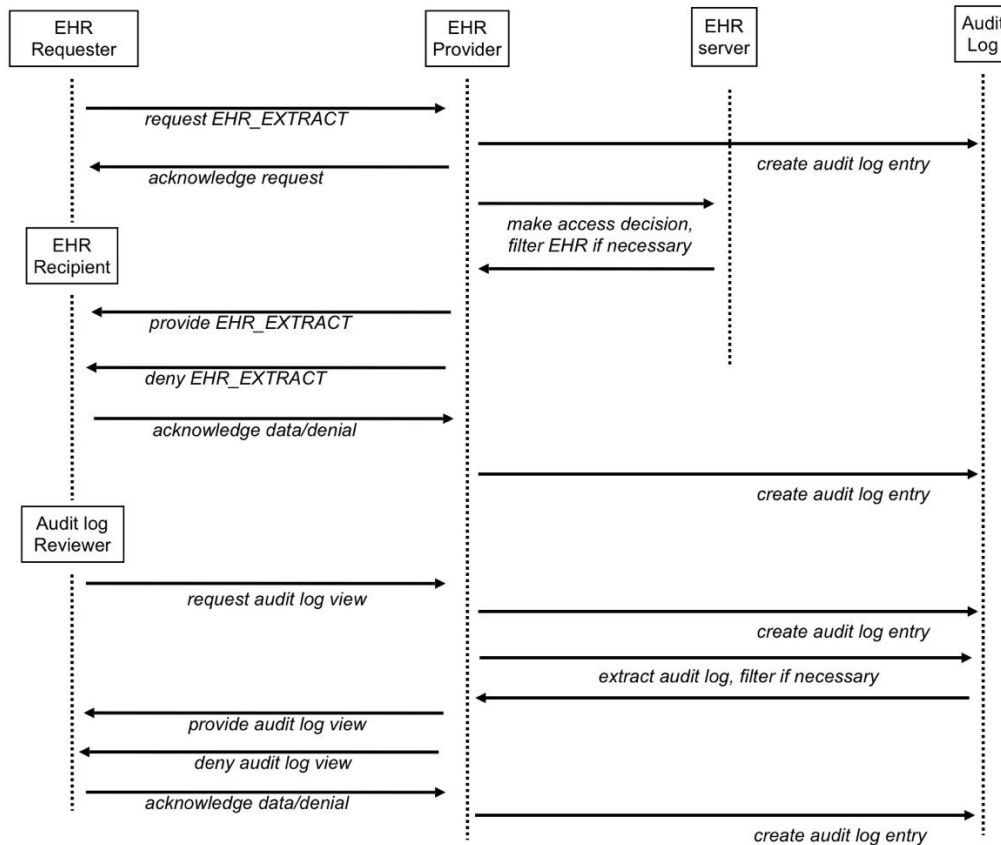


Figure 1 — Principal data flows and security-related business processes covered by this part of EN ISO 13606

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.)

The following subsections describe each data flow in Figure 1.

0.3.2 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 must be sufficient to enable a fully computerised policy negotiation.

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

0.3.3 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 Section 8 of this part of ISO 13606 and the corresponding interface defined in ISO 13606 Part 5.

0.3.4 Acknowledge receipt of EHR_Request

No healthcare-specific security considerations.

0.3.5 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, organisation-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 6 of this part of EN ISO 13606.

0.3.6 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 Part 5.

0.3.7 Provide EHR_EXTRACT

It must be noted 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 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 EN ISO 13606 Part 1, and to the interface model defined in ISO 13606 Part 5.

The EHR_EXTRACT must include or reference any relevant access policies, represented in conformance with this part of EN 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.

0.3.8 Acknowledge receipt of EHR_EXTRACT

No healthcare-specific security considerations.

0.3.9 Generate EHR access log entry

As described in Section 0.2.3 above.

0.3.10 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 an information-sharing 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 his or her EHR within a given EHR system, 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 6 of this part of EN ISO 13606.

The interface model is defined in EN ISO 13606 Part 5.

0.3.11 Generate EHR access log entry

As described in Section 0.2.3 above.

0.3.12 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 6 of this part of ISO 13606.

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 EN ISO 13606 Part 5.

0.3.13 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 EN ISO 13606 Part 5.

0.3.14 Acknowledge receipt of EHR access log view

No healthcare-specific security considerations.

0.3.15 Generate EHR access log entry

As described in Section 0.2.3 above.

0.4 Requirements and technical approach

0.4.1 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 measures 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 (Health informatics – Security management in health using ISO/IEC 27002). This will facilitate the formulation of common security policies across healthcare, and should help promote the adoption of interoperable security components and services. ISO 22600 (Health informatics -- Privilege management and access control) defines a comprehensive architectural approach to formally and consistently defining and managing such policies. 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 must 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 EN ISO 13606. The approach taken in drafting this part of EN 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.

0.4.2 Relationship to other related security standards

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 recognized that vendors and organizations differ in how they have implemented access control policies and services, and the extent to which these are presently computerized.

ISO 22600 (Health Informatics - Privilege Management and Access Control) 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. Figure 2 depicts the concepts of Role Based Access Control defined in ISO 22600.

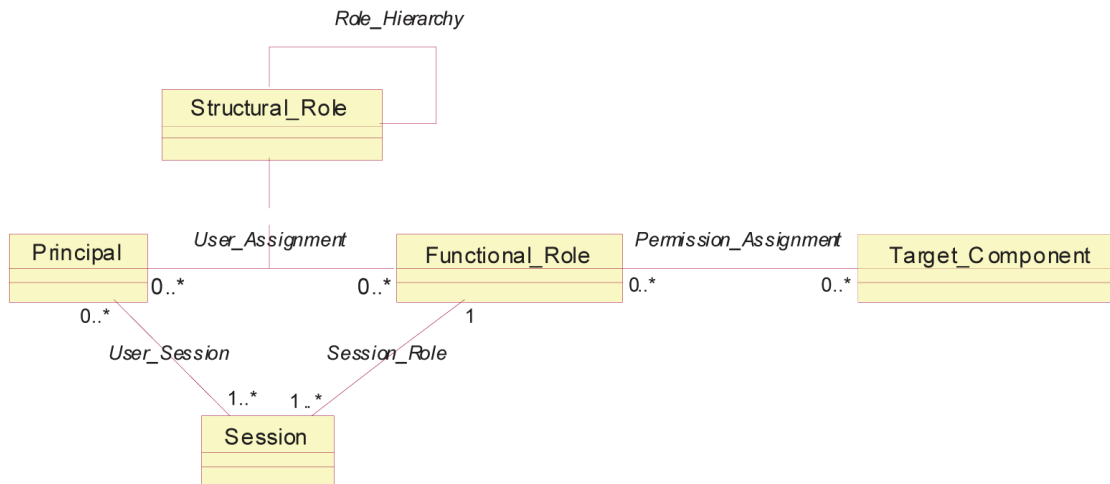


Figure 2 — Main concepts and policy types defined in Role Based Access Control [ISO 22600:2014]

Defining constraints on roles, processes, target objects and related privileges by policies, Figure 2 turns into Figure 3, according to ISO 22600:2014.

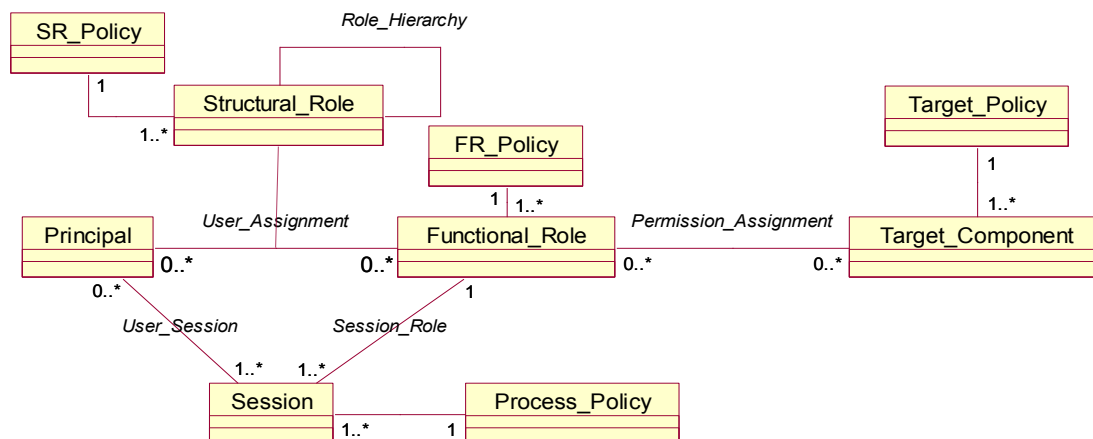


Figure 3 — Policy-driven RBAC Schema

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 Pediatrician 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).

This part of EN ISO 13606 assumes that the ISO 22600 approach is logically applied to govern access decisions in response to an EHR request. For the purposes of this part of EN ISO 13606, the