International Standard

ISO 13606-4

Health informatics — Electronic health record communication —

Part 4: Security

Informatique de santé — Communication du dossier de santé informatisé —

Partie 4: Sécurité

Second edition
2026-08

Reference number
ISO 13606-4:2026(en)

© ISO 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviations ... **2**
5 Conformance ... **2**
6 Record Component Sensitivity and Functional Roles ... **3**
6.1 RECORD_COMPONENT sensitivity ... 3
6.2 Functional roles ... 3
6.3 Mapping of Functional Role to COMPOSITION sensitivity ... 4
7 Representing access policy information within an EHR_EXTRACT ... **4**
7.1 Overview ... 4
7.2 UML representation of the archetype of the access policy COMPOSITION ... 6
7.3 Access policy model properties ... 7
7.3.1 Access policy ... 7
7.3.2 Target ... 7
7.3.3 Request criterion ... 8
7.3.4 Sensitivity constraint ... 9
7.3.5 Attestation information ... 10
7.4 Archetype of the access policy COMPOSITION ... 11
8 Representing audit log information ... **11**
8.1 General ... 11
8.2 EHR audit log extract ... 12
8.3 Audit log constraint ... 12
8.4 EHR audit log entry ... 13
8.5 EHR extract description ... 14
8.6 Demographic extract ... 15
Annex A (informative) **Illustrative access control example** ... **16**
Annex B (informative) **Relations of this document to alternative approaches** ... **20**
Bibliography ... **22**

© ISO 2026 – All rights reserved

Foreword

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

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

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 251, *Health informatics*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO 13606-4:2019 [1]), of which it constitutes a minor revision. The changes are as follows:

— the tables in Clause 7 and Clause 8 have been numbered;

— the examples in Annex B have been anonymized;

— corrections were made to Clause 2 and Clause 3 to reflect the technical content of the document.

A list of all parts in the ISO 13606 [2] series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO 2026 – All rights reserved

Introduction

0.1 General

This document is part of a series including five parts. In this document, dependency upon any of the other parts of this series is explicitly stated where it applies.

0.2 Challenge addressed by this document

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 subjects of care 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 their EHR, as well as the right to be informed of its contents. The communication of health record information to third parties should normally take place only with consent from the subject of care (which can be any freely-given specific and informed indication of their wishes, by which the data subject signifies their agreement to personal data relating to them being processed in an ethically-acceptable way) . More details can be found in ISO 22600-3 [3]. For EHR communication across national borders, ISO 22857 [4] provides guidance that can be used to define appropriate security policy specifications.

Ideally, each fine-grained entry in a subject of care's record should only be accessed by those persons who have permissions to view that information, specified by or approved by the subject of care and reflecting the dynamic nature of the set of persons with legitimate duty of care towards the subject of care through their 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 subject of care feels is too personal for them to access. On the opposite side, the labelling by subjects of care 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 subject of care inappropriately. Subject of care's views on the inherent sensitivity[1)] of entries in their health records can evolve over time, as their personal health anxieties alter or as societal attitudes to health problems change. Subjects of care might wish to offer some heterogeneous levels of access to family, friends, carers and members of their community. Families might 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 subject of care during the course of modern healthcare;

— the large number of healthcare personnel, often rotating through posts, who can potentially come into contact with a subject of care at any one time;

— the large number of healthcare organisations with which a subject of care can come into contact during their lifetime;

— the difficulty (for a subject of care or for anyone else) of classifying in a standardized way how sensitive a record entry can be;

— the difficulty of determining how important a single health record entry can be to the future care of a subject of care, 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 document the term refers only to the characteristic of a resource (EHR data) that implies its value or importance (and by implication the extent of confidentiality and therefore to the functional roles that should have access to it).

© ISO 2026 – All rights reserved

— 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 subjects of care to have their consent for disclosure recorded and respected;

— the low level of concern the majority of subjects of care 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 should be capable of automation. If automated negotiation 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 the overall access decision process 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 subjects of care 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 subject of care'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 document therefore does not prescribe the access rules themselves. 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 [5], and defines specific information structures that are to be communicated as part of an EHR_EXTRACT defined in ISO 13606-1 [5]. Some of the kinds of agreement necessary for the security of EHR communication are inevitably outside the scope of this document, and are covered more extensively in the ISO 22600 [6] series.

It should be noted that there are a number of explicit and implicit dependencies on use of other standards alongside this document, for overall cohesion of an interoperable information security deployment. In addition to agreement about the complete range of appropriate standards, a relevant assurance regime would be required (which is beyond the scope of this document).

0.3 Communication scenarios

0.3.1 Data flows

The interfaces and message models required to support EHR communication are the subject of ISO 13606-5 [7] . 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 are considered by this document. For each key data flow there will be an acknowledgement response, and optionally a rejection may be returned instead of the requested data.

© ISO 2026 – All rights reserved

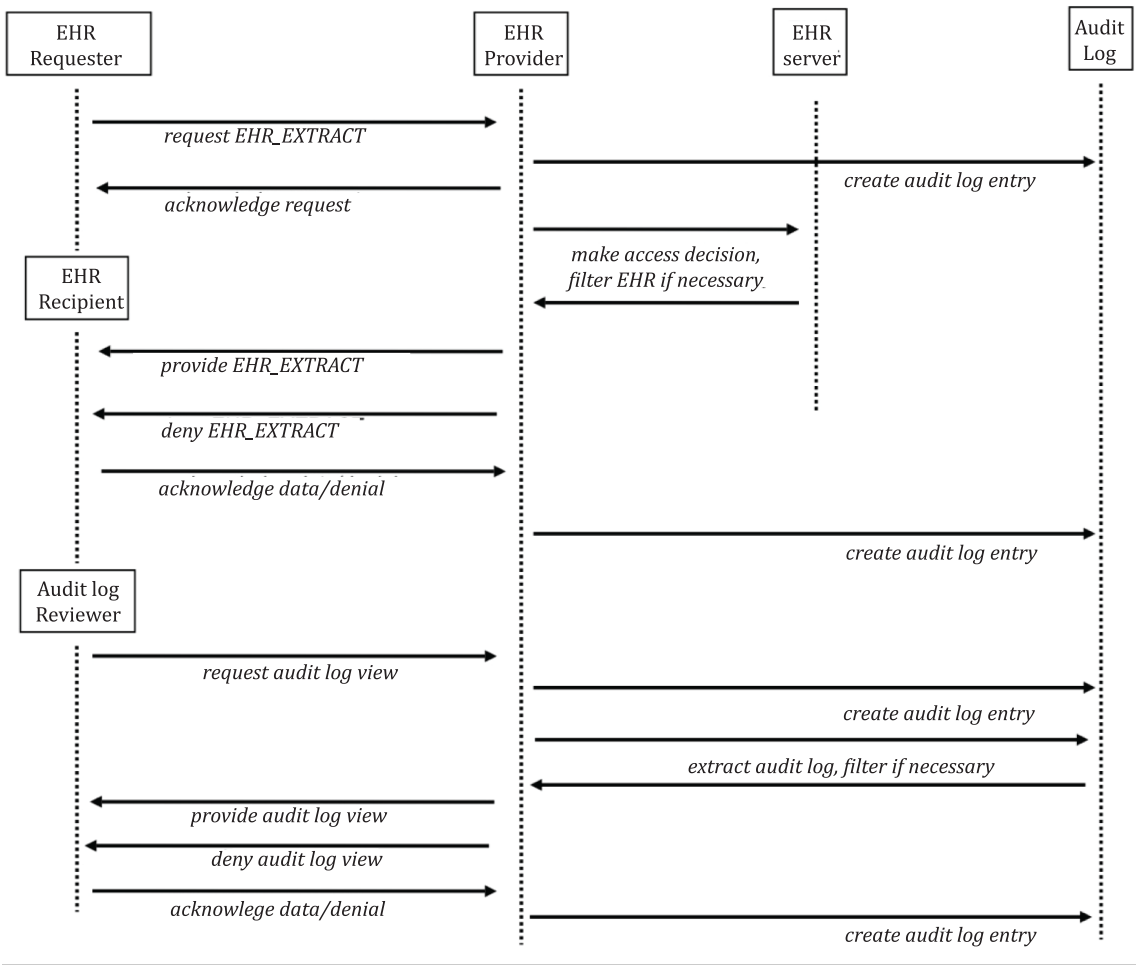


Figure 1 — Principal data flows and security-related business processes covered by this document

The EHR Requester, EHR Recipient and Audit Log Reviewer can be healthcare professionals, the subject of care, a legal representative or another party with sufficient authorization to access healthcare information. Both the EHR_EXTRACT and the audit log, if provided, might 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 (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 subclauses 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 might need to include or reference consents for access and mandates for care, for example by providing some form of explicit consent from the subject of care, or a care mandate.

The negotiation between Requester and Provider of EHR data will increasingly be automated, and the information included in this interaction should be sufficient to enable a fully computerised policy negotiation.

© ISO 2026 – All rights reserved

The requirements for this interaction will be reflected in the REQUEST_EHR_EXTRACT interface model defined in ISO 13606-5 [7].

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 Clause 8 of this document and the corresponding interface defined in ISO 13606-5 [7].

0.3.4 Acknowledge receipt of the 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 document 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 might need to balance the clinical risks of denying access to information with the medico-legal risks of releasing information.

This document 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 subject of care 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 7.

0.3.6 Deny provision of the 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 subject of care.

No healthcare-specific security considerations– the interface model is defined in ISO 13606-5 [7].

0.3.7 Provide the EHR_EXTRACT

It should 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 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 [5], and to the interface model defined in ISO 13606-5 [7].

The EHR_EXTRACT should include or reference any relevant access policies, represented in conformance with this document, 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 0.3.3.

0.3.10 Request EHR access log view

© ISO 2026 – All rights reserved

This is now considered to be desirable practice, to enable a subject of care to discover who has accessed part or all of their EHR in an information-sharing environment. The scope of this interface, as defined in this document, 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.

The interface model is defined in ISO 13606-5 [7].

0.3.11 Generate EHR access log entry

As described in 0.3.3.

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.

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 subject of care or to a healthcare professional might require that some entries are filtered out (such as those referring to EHR data to which the subject of care does not have access).

The interface model is defined in ISO 13606-5 [7].

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 subject of care.

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

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 0.3.3.

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 [8]. 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 [9]. This will facilitate the formulation of common security polices across healthcare, and should help promote the adoption of interoperable security components and services. The ISO 22600 [6] series defines a comprehensive architectural approach to formally and consistently defining and managing such policies. For EHR communication across national borders ISO 22857 [4] provides guidance that can be used to define appropriate security policy specifications.

The exact security requirements that need 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 document. The approach taken in drafting this document 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.

© ISO 2026 – All rights reserved

This document therefore requires that an overall security policy or set of policies conforming to ISO 27799 [9] is in place at all of the sites participating in an EHR communication, and assumes that these policies conform to national or trans-border data protection legislation. Additional policies might be required to conform to specific national, local, professional or organisation regulations applicable to the communication or use of EHR data. Defining such policies is beyond the scope of this document.

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

The ISO 22600 [6] series 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 the ISO 22600 [6] series.

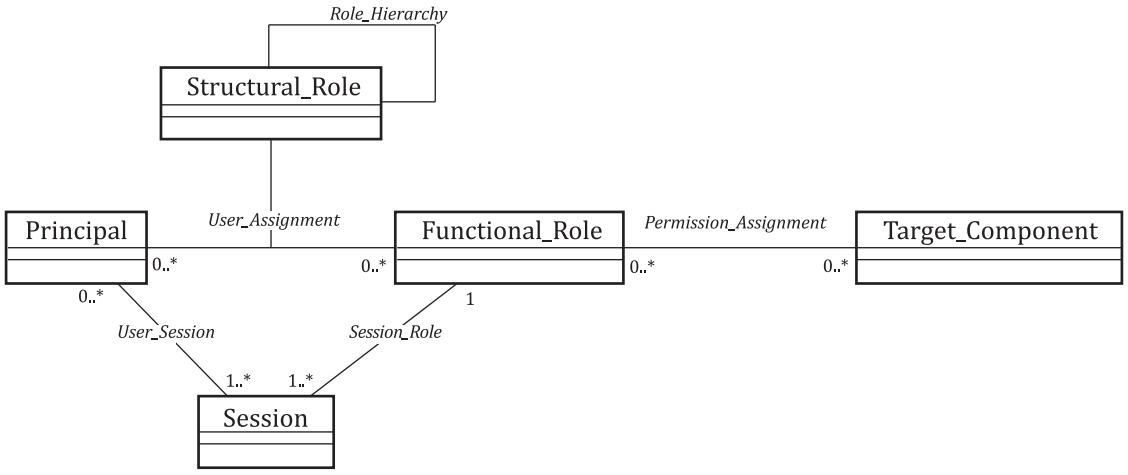


Figure 2 — Main concepts and policy types defined in Role Based Access Control (ISO 22600 [6] series)

Defining constraints on roles, processes, target objects and related privileges by policies, Figure 2 turns into Figure 3, according to the ISO 22600 [6] series.

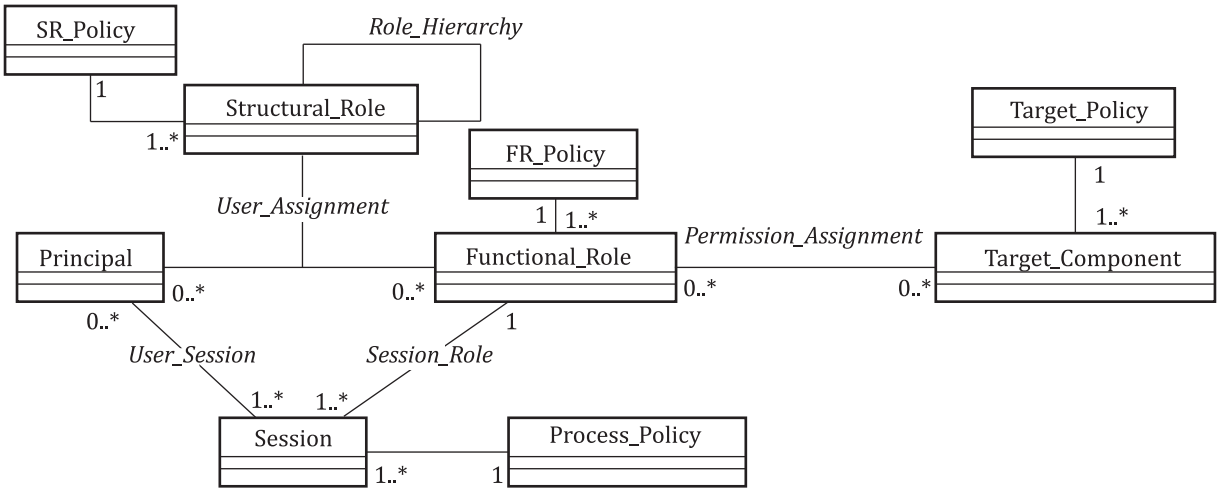


Figure 3 — Policy-driven RBAC Schema

© ISO 2026 – All rights reserved

As illustrated in Figure 3, 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 might hold one or more Structural Roles (such as Consultant Paediatrician at a hospital, Head of Child Screening for the region). Those Structural Roles might permit him or her at times to act with the Functional Role of Personal Clinician to a subject of care. 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 (such as the EHR data which that role-holder is permitted to view).

For the purposes of this document, the Target_Component class shown in Figure 3 is the EHR data held by the EHR Provider. The Permission_Assignment association defines policies to permit or deny access to part or all of the EHR, which need also to be communicated to the EHR Recipient for onward adoption and propagation. Whilst this document assumes the adoption of the ISO 22600 [6] series, it is acknowledged that national operational structures and terminology will differ and that variances will be possible. However, this document only specifies the policy model as a framework to communicate actual access policies in an interoperable way. It does not itself define the content of the access policies that are to be determined at jurisdictional or more local levels.

As a complement to that standard, ISO 21298 [10] define sets of Structural Roles and Functional Roles that can be used internationally to support policy negotiation and policy bridging (for example during the negotiation phase of an access decision). This document also assumes the adoption of ISO 21298 [10], and aligns with it.

The relationship of the policy model defined in this document to the HL7 Healthcare Privacy and Security Classification System is explained in Annex B.

ISO 27789 [11] defines a comprehensive representation of audit log and audit trail information relating to all of the events that can occur within electronic health record systems. This includes the communication of EHR data between repositories and systems. This document assumes conformance to that standard, and defines a profile (sub-set) of the ISO 27789 [11] audit log model specifically for the purpose of communicating with subjects of care and other authorized parties' information about who has accessed the EHR of a specified subject of care, when and why.

A large number of EHR-specific medico-legal and ethical requirements are expressed within ISO 18308 [12], although conformity with these is primarily met through specific classes and attributes of the EHR Reference Model (published in ISO 13606-1 [5]). The ISO 13606 [2] series enables conformity to ISO 18308 [12], and this document specifically enables conformance to its ethical and legal requirements and fair information principles.

05 EHR access policy model

0.5.1 Overall approach

In the ISO 13606-1 [5] Reference Model every COMPOSITION within the EHR_EXTRACT includes an optional access_policy_ids attribute to permit references to such policies to be made at any level of granularity within the EHR containment hierarchy. Every COMPOSITION may 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 the referenced EHR data. The information model in Clause 7 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 some of the main properties of the model are defined as default term lists. Although it is recommended that these be adopted whenever they are suitable, it is recognised that jurisdictions might have requirements or legislation or existing investments that mean that they cannot adopt these internationally-standardised term lists. This document therefore permits jurisdictions to declare conformance using alternative term lists.

Health and care environments increasingly comprise complex networks of agencies and actors from traditional healthcare settings, social care, informal carers and voluntary agencies (such as welfare charities), subjects of care themselves, families and sometimes their social networks. All of these might at times establish agreements to permit data sharing of personal health data. Given the dynamic nature of this "virtual care team" it can be impractical for these data sharing agreements to be negotiated in traditional

© ISO 2026 – All rights reserved

human-to-human, document-based ways. It is therefore likely that such agencies will establish framework agreements that specify in advance the standards they each conform with, any mappings between their respective domains of privilege and how data are to be handled within each such privilege domain. As stated above, this policy model permits jurisdictions to instead declare alternative term lists that they will use. This allows for some flexibility in adoption of this document, recognising that complex data sharing environments might need to establish new, potentially richer, vocabularies to describe the wider range of actors and roles in that environment.

A number of existing and legacy systems might be unable 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 7, this document defines two classifications that can provide a minimum basis for making an access policy decision, and ensure a basic level of access policy interoperability, albeit at a coarse-grained level.

These two vocabularies are:

a) a sensitivity classification of EHR data (at the level of COMPOSITION);

b) a high-level classification of EHR Requesters and Recipients, through a set of Functional Roles.

0.5.2 Defining “need-to-know” when handling EHR data

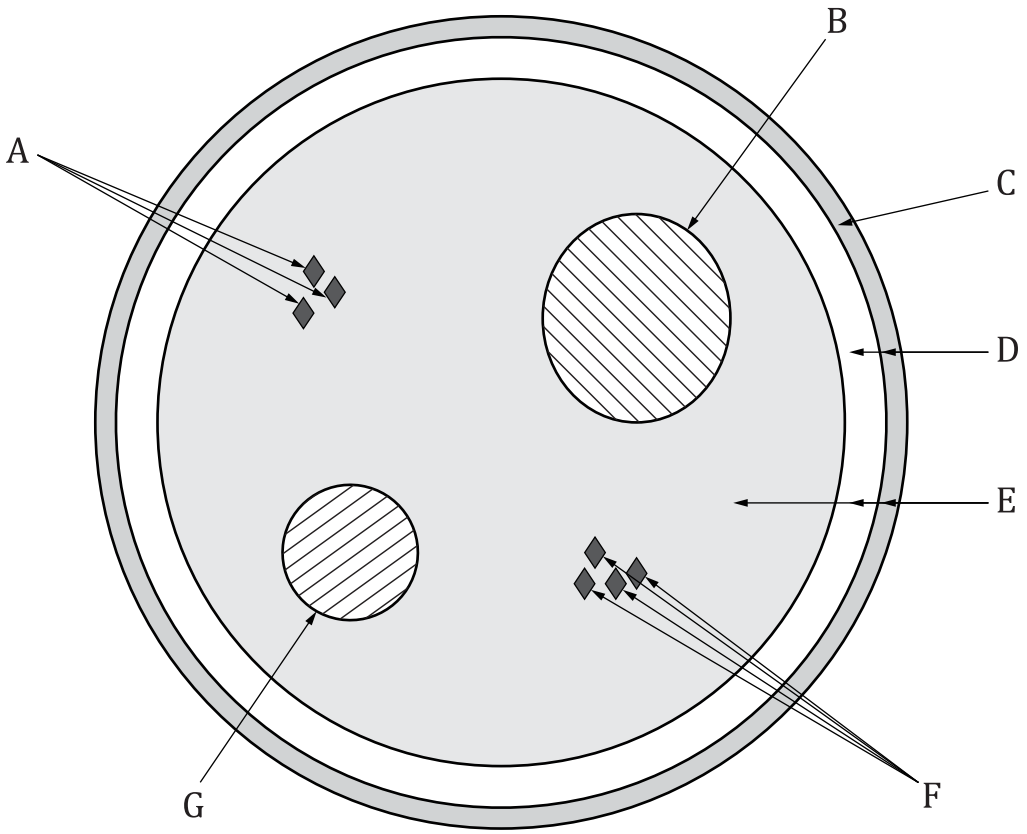
Within many healthcare environments (within and between collaborating healthcare teams involved in the direct provision of care to subjects of care) the norm is to share health record information openly. It is indeed the wish of the vast majority of subjects of care that teams do this, and many subjects of care are actually surprised at how little of their health record is shared today when it should be, for safety and for good continuity of care.

Few contemporary healthcare systems (on paper or electronically) define complex internal access control partitions to the health records that they hold. Even if it were considered useful to define numerous fine-grained access policies, in practice it might take healthcare systems, national health services and millions of subjects of care quite a long time to specify suitable access control policies for all of their EHR data, and to implement software components that can perform many complex policy-bridging computations in real time. Maintenance of these policies as the clinical care requirements of each subject of care evolve would also be a complex process.

While a suite of access policies might in theory be defined (by subjects of care or by others) to provide a multilevel access framework within any given EHR, in practice most clinical settings operate on the basis of default privileges granted throughout the health record to any healthcare or health-related professional who has a legitimate interest in that subject of care. (The definition of who has such a legitimate interest will vary between organisations, and is not the scope of this document.) However, it is also well accepted that subjects of care and professionals might at times need to restrict access to some more personally-sensitive EHR data. It is also common in most health services to ring-fence certain clinical settings as having exclusive portions of an EHR (for example, sexual health clinics).

This kind of ring-fencing of clinical settings or the marking of EHR data as particularly sensitive is quite distinct from any sub-divisions of the EHR that might be defined to assist navigation and workflow within clinical specialties, for example by defining cancer or diabetes portions within the EHR. Figure 4 provides an illustration of the way in which an EHR might logically be subdivided from a need-to-know point of view, in which the confidentiality classification (sensitivity) is represented through classes of user, and for particular care settings.

© ISO 2026 – All rights reserved



Key

A	private entries shared with GP
B	entries restricted to sexual health team
C	entries accessible to administrative staff
D	entries accessible to clinical support staff
E	entries accessible to direct care teams
F	private entries shared with several named parties
G	entries restricted to prison health services

Figure 4 — Access domains within an example EHR

In Figure 4, it is assumed that the subject of care has complete access to their EHR. The majority of this subject of care's EHR is accessible to any party providing direct clinical care. However, the EHR does contain several private entries; some are restricted to the subject of care's general (family) practitioner and some to a separate list of named parties. The EHR also contains some entries created by and restricted to a sexual health clinic, and others restricted to the prison health service – both can only be accessed by parties with relevant additional privilege to that sub-domain (however, the subject of care can nominate other parties to access these subsets of the EHR if they wish). One aspect of privilege is the assignment by an organisation of roles to a clinician that can be exercised in an emergency that confer privileges that exceed those of their normal role. Such an emergency override can, for example, confer access to a wider set of subject of care records than is normally under the care of that clinician (such use of an emergency status would need to be specifically logged and regularly reviewed).

Some parts of the EHR are deliberately also accessible to clinical support staff, who might need to review certain clinical findings in order to perform tasks such as planning or performing investigations. A very small part of this example EHR has also been made accessible to administrative staff. Appointments clerks, secretaries and porters all need to know certain key facts about a subject of care in order to play their role in the overall delivery of efficient care, such as knowing that a subject of care has special health advocacy needs or that they will need to have 24 % oxygen and a wheelchair in order to be transported to the radiology department.

© ISO 2026 – All rights reserved

This example does not illustrate how subjects of care can be excluded from access to portions of the EHR, but such stipulations can be made using the generic policy framework of Clause 7, if permitted under data protection legislation. An example of this will be if the EHR data was provided in confidence by a relative of the subject of care.

While a set of rich policies can be defined for specific kinds of subjects of care, specific settings, or in cases where subjects of care have specific concerns about their EHR, the adoption of distributed EHR solutions needs to be managed on the basis that a sensible set of defaults and a simple framework will satisfy the majority of cases in the near future. This is because a rich set of policies might not be capable of direct interpretation and incorporation within the EHR system of an EHR Recipient, even if the information in those policies can be communicated in a standardized way.

In addition to the generic representation of EHR access policy information, this document therefore also defines a specification for a minimum basis for communicating the sensitivity of EHR data within an EHR_EXTRACT, by specifying the sensitivity of the COMPOSITIONs within it according to the classification defined in 6.1. This classification corresponds to the various sub-domains of EHR data illustrated in Figure 4.

In practice any given EHR system might have other mechanisms for indicating the sensitivity of EHR data or some equivalent concept. This document does not require EHR systems to store data according to the sensitivity levels defined in 6.1, but to be able to map to this classification on generating an EHR_EXTRACT.

0.5.3 Functional Roles for accessing EHR data

In order to make an access decision, the profile and purpose of a proposed EHR Recipient need to be matched to the policies applying to the EHR held by the EHR provider, including the sensitivity of the specific RECORD_COMPONENTS that have been requested.

The profile of the Requester or Recipient, or both, therefore needs to be specified in an interoperable way. As discussed earlier, the requirements, legislation, attributes and vocabularies used for describing requester profiles in each country vary, and cannot yet be standardized.

However, in order to provide a basic level of interoperability, minimum conformance to this document does require either that any request for an EHR_EXTRACT include, as part of the request specification, the Functional Role of the intended EHR Recipient, as defined in 6.2 and corresponding to those defined in ISO 21298 [10], or that an alternative jurisdictionally-specified term list be used.

The correlation between Functional Role and EHR sensitivity, for the purpose of granting or denying an access request, or for filtering the EHR_EXTRACT, is defined in 6.3.

This mapping provides a basic (coarse-grained) way of limiting the scope of EHR access according to the kind of party who is making the access request. Additional details can always be added in situations for which an interoperable specification of the Requester profile has been defined at a local or national level. An illustration of the way in which this basic mapping can be combined with a small number of additional specifications to specify a relatively rich set of access constraints is provided in Annex A.

0.6 Audit log interoperability

It is widely recognized that the details of interactions with an EHR system need to be retained for auditability purposes. However, the way in which these kinds of audit logs are implemented is quite specific for each EHR system, partly determined by the persistence (such as database storage) approach adopted, and can also partly be directed by local or national legislation.

Requirements for EHR audit trails are specified in ISO 27789 [11], which specifies a common framework for audit trails for EHRs, in terms of audit trigger events and audit data, to keep the complete set of personal health information auditable across information systems and domains.

However, there is increasing evidence that the ability for subjects of care to review information about access to their EHR data is not only a legitimate right but actually helps encourage moral behaviour amongst healthcare professionals in accessing only the records they genuinely need to see. Whilst individual EHR systems can provide some degree of access to the audit log, this is at present usually provided to database administrators using tools and interfaces that are unsuitable for permitting subjects of care to browse their

© ISO 2026 – All rights reserved

own EHR's access history. In a distributed (shared) EHR scenario, the EHR, and logs of accesses to it, are inevitably distributed too.

An interoperable specification is therefore required for a basic set of data that can be provided in response to a request (by a subject of care or their representative) to provide a list of accesses to the EHR (held within an EHR system). This basic data set is therefore defined both as an audit log review information model in this document and as a request and response interface model in ISO 13606-5 [7]. Since future EHR systems and audit logging systems will increasingly conform to ISO 27789 [11], and can therefore have internal data models and/or interfaces that reflect its structure, the audit log model in Clause 8 of this document includes mapping information to ISO 27789 [11]. Not all properties of the audit log model in this document have correspondence with ISO 27789 [11], as some details describing the kind of EHR data accessed will need to be taken from the EHR system itself.

This audit log view is not intended as the means by which an audit log is examined as part of a formal investigation of accesses to an EHR system, nor for interoperable communications between audit trail systems.

© ISO 2026 – All rights reserved

Health informatics — Electronic health record communication —

Part 4: Security

1 Scope

This document describes a methodology for specifying the privileges necessary to access electronic health record (EHR) data. This methodology forms part of the overall EHR communications architecture defined in ISO 13606-1 [5].

This document seeks to address those requirements uniquely pertaining to EHR communications and to represent and communicate EHR-specific information that will inform an access decision. It also refers to general security requirements that apply to EHR communications and points to technical solutions and standards that specify details on services meeting these security needs.

NOTE Security requirements for EHR systems not related to the communication of EHRs are outside the scope of this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 13606-1, *Health informatics — Electronic health record communication — Part 1: Reference model*

ISO/TS 14265, *Health informatics — Classification of purposes for processing personal health information*

ISO 21298, *Health informatics — Functional and structural roles*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 13606-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
authority
entity responsible for the issuance of certificates

Note 1 to entry: Two types of authority are distinguished in this document: certification authority, which issues public-key certificates, and attribute authority, which issues attribute certificates.

3.2
identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

© ISO 2026 – All rights reserved

3.3
functional role
role which is bound to an act

Note 1 to entry: Functional roles can be assigned to be performed during an act.

[SOURCE: ISO 21298:2017 [13], 3.9, modified — Notes 2 and 3 to entry have been removed.]

3.4
policy
set of legal, political, organizational, functional and technical obligations for communication and cooperation

[SOURCE: ISO 22600-1:2014 [14], 3.13]

3.5
privilege
capacity assigned to an entity by an *authority* (3.1)

[SOURCE: ISO 22600-1:2014 [14], 3.17, modified — "according to the entity's attribute" was removed from the definition.]

3.6
sensitivity
characteristic of a resource that implies its value or importance

[SOURCE: ISO 22600-2:2014 [15], 3.37]

4 Abbreviations

For the purposes of this document, the following abbreviations apply.

EHR	electronic health record
EU	European Union
GP	general practitioner
HL7	Health Level Seven
PMAC	privilege management and access control
UML	unified modelling language
XML	extensible mark-up language

5 Conformance

This document requires conformance to one of two principal provisions:

— using a coarse-grained minimum approach to specify sensitive EHR data and the functional role of the Recipient, used as a basis for making an access decision;

— using a generic policy model to communicate detailed access policy information reflecting the disclosure wishes of the subject of care and/or local or national guidelines that need to be shared as part of the process of EHR distribution.

It optionally includes conformance to an interoperable audit log view specification.

For minimum conformance, the sensitivity of the RECORD_COMPONENTS within an EHR_EXTRACT shall be provided according to the classification defined in 6.1. Any request for an EHR_EXTRACT shall include, as part of the request specification, the Functional Role of the intended EHR Recipient, as defined in 6.2. The

© ISO 2026 – All rights reserved