INTERNATIONAL STANDARD

ISO 13606-4

First edition
2019-06

Health informatics — Electronic health record communication —

Part 4: Security

Informatique de santé — Communication du dossier de santé informatisé —

Partie 4: Sécurité

Reference number
ISO 13606-4:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

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).

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 (see 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 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health Informatics*.

This first edition of ISO 13606-4 cancels and replaces the first edition of ISO/TS 13606-4:2009, which has been technically revised. The main changes compared to the previous edition are as follows:

— Functional Roles

  — Some terms for functional roles have been updated to align with CONTSYS.

  — The rules for using this vocabulary now state that jurisdictions can nominate alternatives or specialisations of these terms if needed.

— Access policy model

  The access policy model now also permits jurisdictional alternative terms to be used where appropriate.

— Audit log model

  The audit log model now aligns with the ISO 27789 standard for EHR audit trails. It contains more information than is present in ISO 27789: it is a kind of specialisation specifically dealing with the communication of EHR information and audit log information. It therefore includes information about the EHR extract or the audit log extract being communicated, which is beyond the scope of ISO 27789.

A list of all parts in the ISO 13606 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.

Introduction

0.1 General

This document, is part of a five-part standard series, published jointly by CEN and ISO through the Vienna Agreement. 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 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 can 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 can 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 sensitivity[1)] of entries in their health record can 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 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 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 organisations 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;

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 access controls.

— 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 to receive the data should 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 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, and defines specific information structures that are to be communicated as part of an EHR_EXTRACT defined in ISO 13606-1. 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 ISO 22600 (Privilege Management and Access Control).

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. 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 document. For each key data flow there will be an acknowledgement response, and optionally a rejection may be returned instead of the requested data.

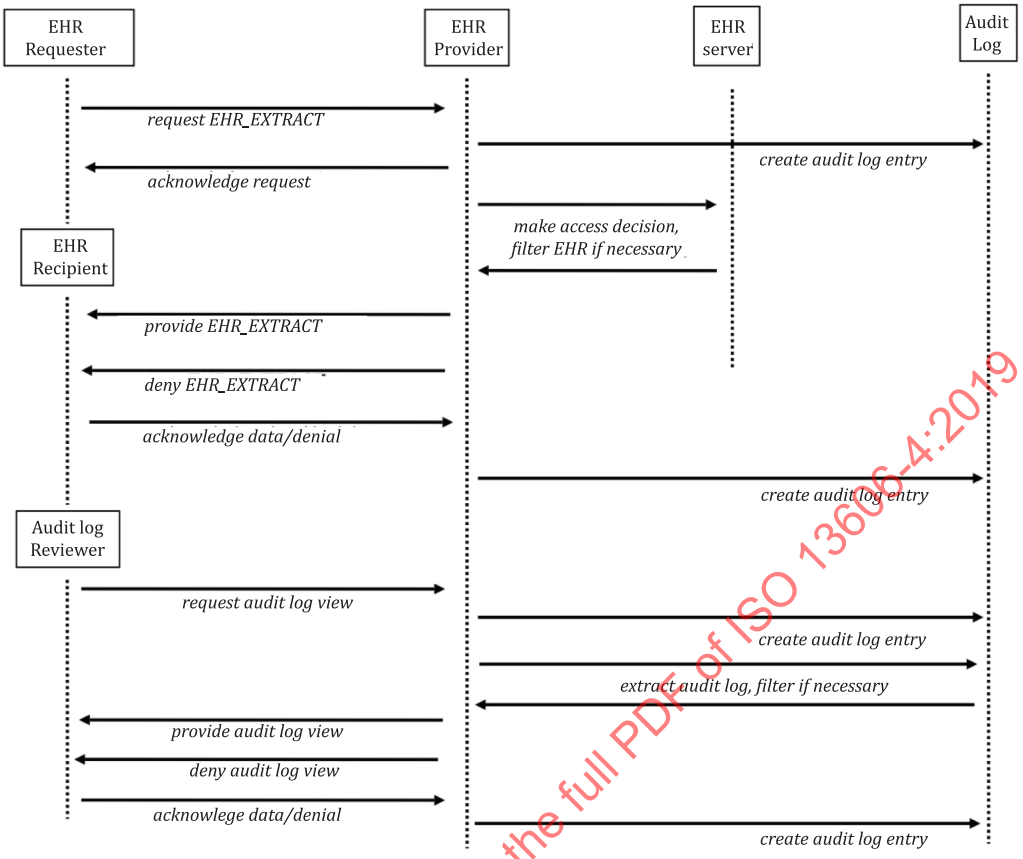


Figure 1 — Principal data flows and security-related business processes covered by this document

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, 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 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 should be sufficient to enable a fully computerised policy negotiation.

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

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

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 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 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 patient.

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

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 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 sh 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

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 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.

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

The interface model is defined in ISO 13606-5.

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 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. 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 polices 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 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.

This document therefore requires 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 polices 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.

ISO 22600 (all parts) 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 (all parts).

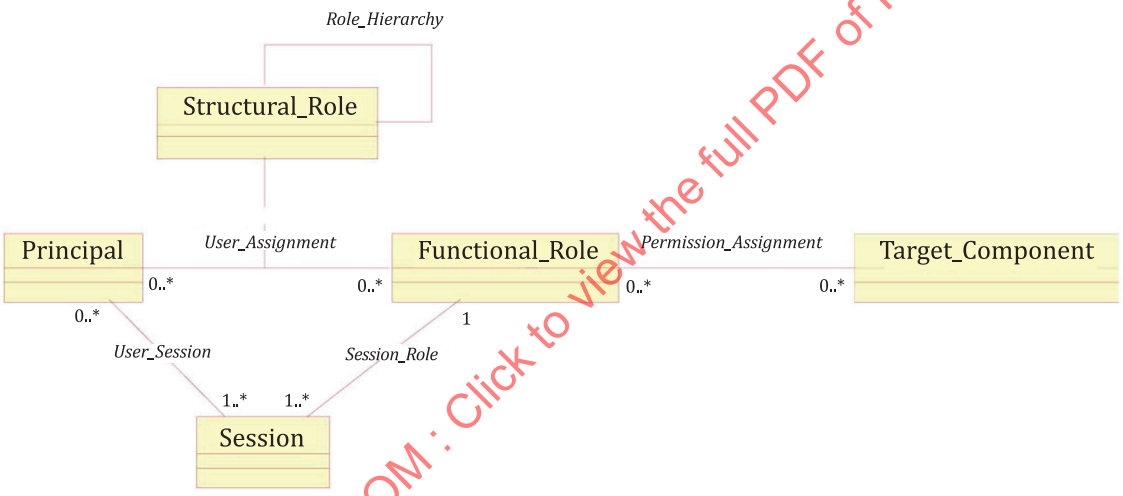


Figure 2 — Main concepts and policy types defined in Role Based Access Control [ISO 22600 (all parts)]

Defining constraints on roles, processes, target objects and related privileges by policies, Figure 2 turns into Figure 3, according to ISO 22600 (all parts).

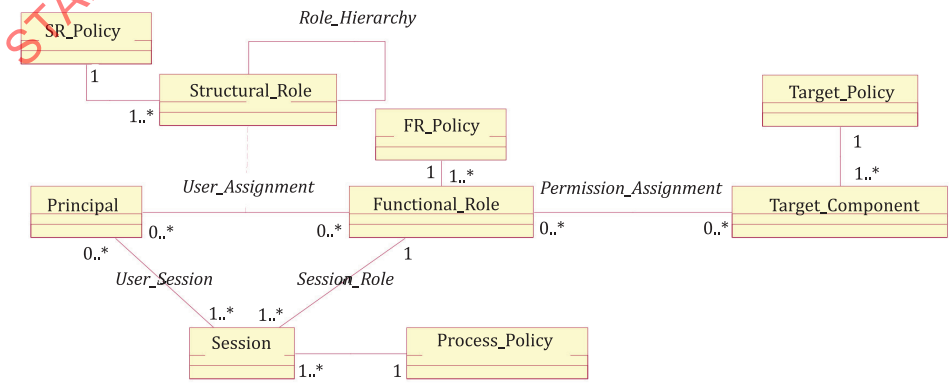


Figure 3 — Policy-driven RBAC Schema

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 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 (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 that standard 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 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 that standard, 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 defines a comprehensive representation of audit log and audit trail information relating to all of the events that might 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 audit log model specifically for the purpose of communicating with patients and other authorised parties' information about who has accessed the EHR of a specified patient, when and why.

A large number of EHR-specific medico-legal and ethical requirements are expressed within ISO 18308, although compliance with these is primarily met through specific classes and attributes of the EHR Reference Model (published in ISO 13606-1). The ISO 13606 standard as a whole enables conformance to ISO 18308, 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 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 it. 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) patients 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 might not be practical for these data sharing agreements to be negotiated in traditional 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 comply 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 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 7, this document 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:

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.

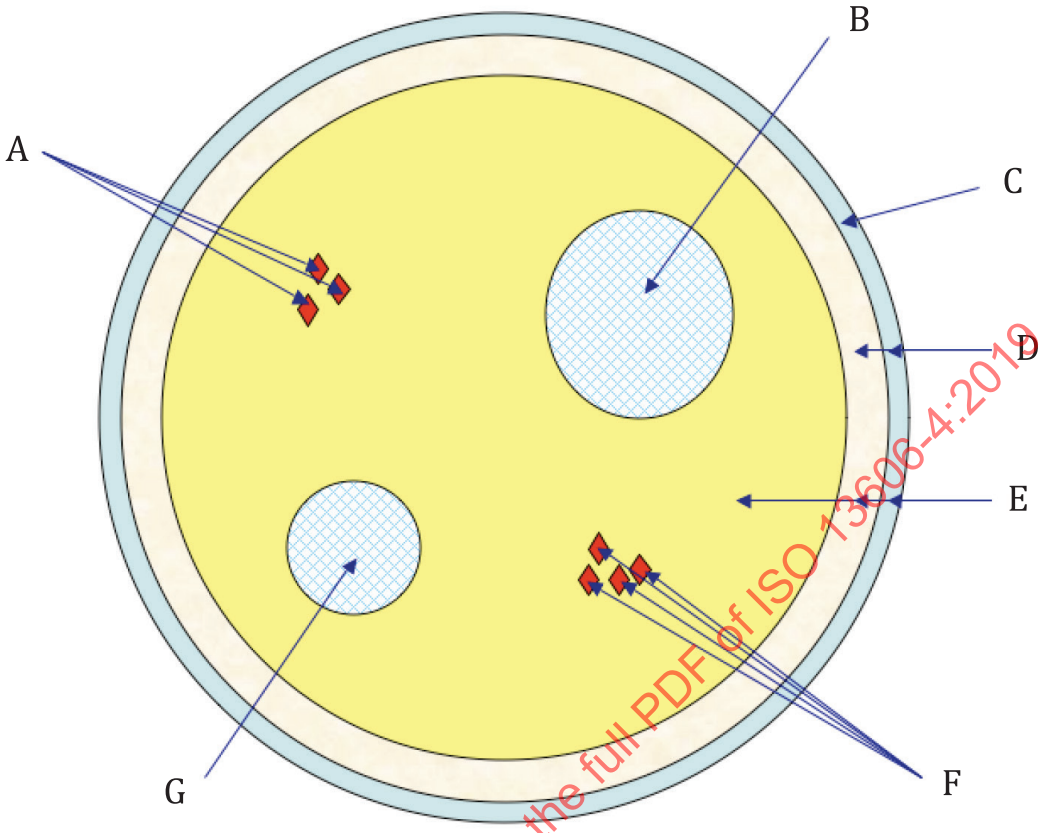
0.5.2 Defining 'Need to Know' when handling EHR data

Within many healthcare environments (within and between collaborating healthcare teams involved in the direct provision of care to patients) the norm is to share health record information openly. It is indeed the wish of the vast majority of patients that teams do this, and many patients 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 health care systems, national health services and millions of patients 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 patient evolve would also be a complex process.

Whilst a suite of access policies might in theory be defined (by patients or by others) to provide a multi-level access level 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 patient. (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 patients 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.



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 — Illustration of access domains within an example EHR

In this illustration, it is assumed that the patient has complete access to his or her EHR. The majority of this patient's EHR is accessible to any party providing direct clinical care. However, the EHR does contain several private entries; some are restricted to the patient'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 patient might nominate other parties to access these subsets of the EHR if he or she wishes). One aspect of privilege is the assignment by an organisation of roles to a clinician that might be exercised in an emergency that confer privileges that exceed those of his or her normal role. Such an emergency override might, for example, confer access to a wider set of patient 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 have need to know certain key facts about a patient in order to play

their role in the overall delivery of efficient care, such as knowing that a patient has special health advocacy needs or that he will need to have 24 % oxygen and a wheelchair in order to be transported to the radiology department.

This example does not illustrate how patients 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 patient.

Whilst a set of rich policies might be defined for specific kinds of patients, specific settings, or just because one patient is more concerned about his or her EHR than another, 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 and/or recipient therefore needs to be specified in an interoperable way. As discussed earlier, the requirements, legislation, attributes and vocabularies used for this 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, 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 s 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 sophistication 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 might 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 might also partly be directed by local or national legislation.

Requirements for EHR audit trails are specified in ISO 27789:2013 Health informatics – Audit trails for electronic health records. That standard 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 patients to be able 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 might be able to 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 patients to browse their 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 patient or his/her representative) to provide a list of accesses to the EHR (held within an EHR system). This 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. Since future EHR systems and audit logging systems will increasingly conform to ISO 27789, and might 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. Not all properties of the audit log model in this document have correspondence with ISO 27789, 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.

Health informatics — Electronic health record communication —

Part 4: Security

1 Scope

This document describes a methodology for specifying the privileges necessary to access EHR data. This methodology forms part of the overall EHR communications architecture defined in ISO 13606-1.

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 at 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*

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 terminological databases for use in standardization at the following addresses:

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

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

3.1
authority
entity, which is responsible for the issuance of certificates.

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

3.2
availability
property of being accessible and useable upon demand by an authorized entity

[SOURCE: ISO 7498-2:1989]

3.3
identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

3.4
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, 3.9]

3.5
policy
set of legal, political, organizational, functional and technical obligations for communication and cooperation

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

3.6
privilege
capacity assigned to an entity by an *authority* (3.1)

[SOURCE: ISO 22600-1:2014, 3.17]

3.7
sensitivity
characteristic of a resource that implies its value or importance

[SOURCE: ISO 22600-2:2014, 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
ISO	International Organization for Standardization
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 needs 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 correlation between Functional Role and EHR sensitivity, for the purpose of granting or denying an access request, or for filtering the EHR_EXTRACT, shall comply with the mapping defined in 6.3.

Normal Conformance to this document, the EHR_EXTRACT shall contain or reference a generic representation of any policy information relating to the EHR data being communicated, either logically according to 7.2 in conjunction with any other published standard for access policy representation, or explicitly according to 7.3. A policy may alternatively be referenced and not included within the EHR_EXTRACT if the EHR Provider is assured that the EHR Recipient already has direct access to the same policy information. Normal Conformance may optionally specify an obligation to comply with Minimum Conformance.

Extended Conformance, if an interoperable audit log view is required, in additional to Normal Conformance, the information model in Clause 8 shall be used to represent that view.

6 Record Component Sensitivity and Functional Roles

6.1 RECORD_COMPONENT sensitivity

Within an EHR_EXTRACT as defined by ISO 13606-1, the sensitivity[2)] of each COMPOSITION, if specified, will be one of the values for CS_SENSITIVITY defined in Table 1.

Table 1 — Values of CS_SENSITIVITY to be used for the sensitivity attribute of COMPOSITION

CS_SENSITIVITY value	Sensitivity level	Description of intended access to COMPOSITIONs of this sensitivity
Personal	5	Confidential to the subject of care, and to be shared perhaps with a few key persons whom they trust most, or only accessible to the subject of care (and to others by one-off authorizations)
Privileged care	4	Access restricted to a small group of people caring intimately for the patient, perhaps an immediate care team or senior clinical party (the privileged clinical setting needs to be specified such as mental health)
Clinical care	3	Default for normal clinical care access (most clinical staff directly caring for the patient should be able to access nearly all of the EHR)
Clinical management	2	Less sensitive COMPOSITIONs, that might need to be accessed by a wider range of personnel not all of whom are actively caring for the patient (such as radiology staff)
Care management	1	COMPOSITIONs that might need to be accessed by a wide range of administrative staff to manage the subject of care's access to health services

6.2 Functional roles

The functional role of any intended EHR Recipient shall be one of the values for Functional Role defined in Table 2, unless an alternative and/or enriched set of roles has been agreed between communicating parties and is used for normal conformance to this document. The roles defined here are aligned with the functional roles defined in ISO 21298.

2) 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 access controls.

Table 2 — List of Functional Roles

Functional Role	Brief description
Subject of care	principal data subject of the electronic health record.
Subject of care proxy	for example, parent, guardian, carer, or other legal representative NOTE Some jurisdictions can use different terms to describe this role.
Personal healthcare professional	healthcare professional or professionals with the closest relationship to the patient, often the patient's GP.
Privileged healthcare professional	nominated by the subject of care; OR nominated by the healthcare facility of care (if there is a nomination by regulation, practice, etc. such as an emergency over-ride).
Directly involved healthcare professional	'healthcare professional involved in providing direct care to the subject of care.
Indirectly involved healthcare professional	healthcare professional indirectly involved in patient care (teaching, research, etc.).
Supporting healthcare party	any other parties supporting service provision to the subject of care.

6.3 Mapping of Functional Role to COMPOSITION sensitivity

When making an access decision, at minimum Table 3 shall be used to determine the sensitivities of COMPOSITION to which an EHR Recipient may be granted access according to the Functional Role defined in the EHR Request.

Table 3 — Mapping of Functional Roles to COMPOSITION sensitivity

Functional Role	COMPOSITION sensitivity				
	Care management	Clinical management	Clinical care	Privileged care	Personal care
Subject of care	Y	Y	Y	Y	Y
Subject of care proxy	Y	Y	Y	Y	Y
Personal healthcare professional	Y	Y	Y	Y	Y
Privileged healthcare professional	Y	Y	Y	Y+	++
Directly involved healthcare professional	Y	Y	Y		
Indirectly involved healthcare professional	Y	Y			
Supporting healthcare party	Y				

NOTE 1 Y indicates that access will be granted to COMPOSITIONs of this sensitivity unless otherwise dictated by other policy constraints as specified according to Clause 7.

NOTE 2 + Indicates that access will be granted if the EHR Recipient is a member of the same speciality or clinical service as that in which the COMPOSITION was created such as sexual health clinic, prison health service. This access can also be granted in health care emergency situations if so authorized.

NOTE 3 ++ Indicates that access to personal care information can sometimes be granted by mandate to Privileged Healthcare Professionals in some care settings, such as in the armed forces of some countries.

7 Representing access policy information within an EHR_EXTRACT

7.1 Overview

Within an EHR_EXTRACT, the access policy information to be communicated to the EHR Recipient is represented as one or more COMPOSITIONS within a dedicated *Access policies* FOLDER. This specification is not intended to represent the way in which software components might represent this

kind of information within an EHR system or within security components supporting the EHR system. It is intended to be a generic way of including this information within an EHR_EXTRACT so that the EHR Recipient is able to continue to respect the same consent wishes in any onward propagation or access to the EHR data (it should be noted that COMPOSITIONS can be attested, and proof of that attestation included within the EHR_EXTRACT). The entire FOLDER is optional, as it might not always be necessary to exchange policy information between parties, for example if they already have common access to such policy information, or if no unique policies have been defined for that particular EHR.

Each policy is represented as a single COMPOSITION, whose archetype shall conform to or specialize the reference archetype named Access_policy_rule published in ISO 13606-3. Each instance of this is a kind of policy extract, and would be created to communicate a discrete specification of permission or denial to access part or all of an EHR, and which is considered appropriate to include within an EHR_EXTRACT for future use by the EHR Recipient. In order to simplify the process of conforming to ISO 13606 as a whole, information about the authorship, creation, version history and attestation of access policy information is represented in the same way as for other COMPOSITIONs within an EHR_EXTRACT.

Because access policies are intended to be communicated as COMPOSITIONs conforming to ISO 13606-1, the instances of a policy can be version-managed and attested as any other COMPOSITION. It is possible, for example, to include or reference the signature of the subject of care relating to an access policy or to indicate that an access policy is a replacement for one previously communicated.

An EHR_EXTRACT may be used exclusively to communicate access policy information, without any other EHR data, if appropriate. The policy information model, represented logically as specified in 7.3, may instead be represented and communicated more generally as an ISO 22600-3 (PMAC) policy, which fully complies with the Interoperability Reference Architecture Model of ISO 13606-1, Annex C.

The Access_policy_rule COMPOSITION archetype comprises four ENTRYs including properties to represent the effective start and end times of the policy, if these are specified. (If start and end times are not specified the policy is deemed to apply indefinitely, from the date and time when it was created.)

The REQUEST_CRITERIA ENTRY is used to define the kind of request scenario to which this policy applies. The kind of request might be specified in terms of a particular profile of Functional Role, Structural role, Clinical setting or Specialty or Purpose of use. Individual actors (such as persons, organisations, devices, agents) might be identified, through an instance identifier that can be mapped to a fuller description of the party in the DEMOGRAPHIC_EXTRACT (as defined in ISO 13606-1). Each of these ways of defining the request scenario is represented as a list of one or more ELEMENTS within a containing ENTRY. For one instance of REQUEST_CRITERIA, the properties are intended to be applied as AND criteria. For example, using structural_role, care_setting and purpose it is possible to define a policy that only applies to any “psychiatrist” and working in an “adolescent care unit” and for the purpose of “research”. These criteria would NOT apply separately (a) to any psychiatrist or (b) to any staff in an adolescent care unit or (c) for anyone conducting research. If an access policy contains more than one instance of REQUEST_CRITERIA then these are to be applied as OR: an actual request that fits any of the criterion set instances should trigger the application of this policy rule.

The TARGET ENTRY is used to define the parts of the EHR to which the policy applies. The parts of the EHR can be defined very specifically, for example as the rc_id of one particular FOLDER or as a list of particular RECORD_COMPONENTS (for example, some of those being communicated within the same EHR_EXTRACT). Alternatively, the parts of the EHR can be specified by a set of archetypes, and/or by time period. This permits, for example, a policy to be specified as applicable to all microbiology reports created between 2003 and 2005. Other selection criteria may also be included, as constraints expressed as strings. As for REQUEST_CRITERIA, the list of ELEMENTS within an ENTRY form a union set (AND) and the set of ENTRYS within the TARGET SECTION form an intersection set (OR).

The SENSITIVITY_CONSTRAINTS ENTRY is used to define the permissions that apply to requests matching the REQUEST_CRITERIA for data that matches the TARGET specification. For minimum conformance to this document, the properties of this class are used to represent the applicable values from Table 1. Up to four values from Table 1 may be included for minimum conformance to this document, to represent the maximum sensitivity value that permits each of the four types of processing specified (access, write, modify, communicate). At its simplest level, the rule might be to permit or deny full access to the target data. However, to offer some flexibility, the SENSITIVITY_CONSTRAINTS

ENTRY archetype represents the permission as an integer indicating the maximum sensitivity to which access is granted. The sensitivity level corresponds to the values given in Table 1 of this document. If an integer value of 1 is specified, this implies that full access is granted to the specified parts of the EHR, whilst a value of 6 would indicate complete denial of access. The SENSITIVITY_CONSTRAINTS ENTRY archetype distinguishes an integer value for access to existing EHR data, a value for the maximum sensitivity at which new data may be created, a maximum value of data that may be modified, and a maximum value for which the recipient may elect to further share the data. This set of four rules would permit, for example, an EHR Recipient to have read-only access to the EHR data, with no permissions to share it with anyone else, or permit a Recipient to read but not change the existing data and to add new data to that part of an EHR.

Another part of the SENSITIVITY_CONSTRAINTS ENTRY is used to specify if access is granted to all historic versions of the EHR data or only to the current (most recent) version. This might need to be specified in some access policies in order to comply with data protection legislation.

Other rules can be specified as strings. If other string specifications are used, when adopting normal conformance to this document, it will be for an EHR-sharing community to ensure that these are mutually interpretable by humans and/or by computers.

The overall aim of this COMPOSITION archetype is to permit the representation of basic access policy information in a simple and interoperable way, whilst also permitting more sophisticated rules to be included and communicated. However, in order for more complex rules to be usefully included, the EHR Provider have to be satisfied that the EHR Recipient is able to understand and accommodate those additional rules.

It should be remembered that this representation is for the purpose of communicating EHR policy information as part of the EHR_EXTRACT, and is not intended as the policy model within security components nor for the exchange of policy information between security systems.

7.2 UML representation of the archetype of the access policy COMPOSITION

The UML diagram in Figure 5 is a logically equivalent representation to the Reference Archetype specified in ISO 13606-3. The UML representation is the logical representation for conformance in this document to support the communication of access policy information according to ISO 22600 (all parts).

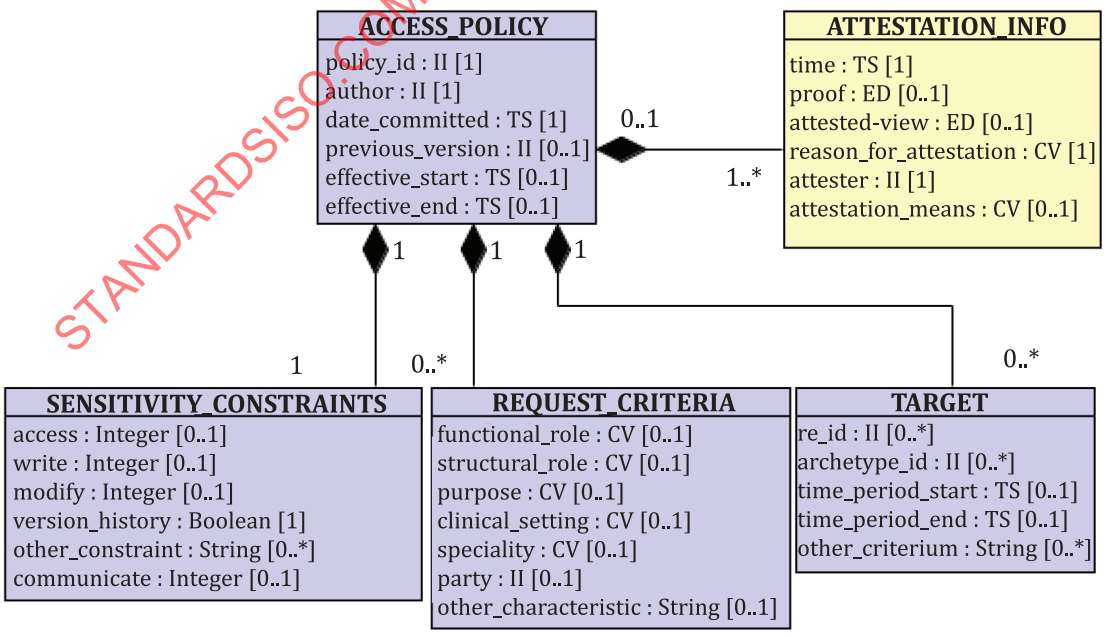


Figure 5 — UML representation of the access policy model

Access policy model properties

7.2.1 Access policy

Term: access policy

Definition: Representation of the rules specified within a single access policy

Class name: ACCESS_POLICY

Description: This is the root class of the access policy model, used to represent a discrete specification of permissions or denials to process part or all of an EHR (the rules within a policy), for communication within an EHR_EXTRACT or through some other agreed format and channel.

Attributes

#	Attribute name	Datatype	Description
1	policy_id	II[1]	The unique identifier of this policy, which may be referenced from COMPOSITION instances within an EHR_EXTRACT
2	author	II[1]	The unique identifier of the person responsible for creating this policy, which might be the patient, a related party, a healthcare professional or another authorised person. The identifier may correspond with a person (in a role) specified within the DEMOGRAPHIC_EXTRACT.
3	date_committed	TS[1]	The date and time when the information specified in this policy model was first committed to a system or service or repository from which it could function.
4	previous_version	II[0..1]	The policy_id of an instance of a policy that this policy replaces.
5	effective_start	TS[0..1]	The data and time at which this policy was or is first intended to apply.
7	effective_end	TS[0..1]	The data and time at which this policy was or is intended to cease being valid.

Relationships

#	Class name		Aggregation of	
1	1	ACCESS_POLICY	1	SENSITIVITY_CONSTRAINTS
2	1	ACCESS_POLICY	0..*	TARGET
3	1	ACCESS_POLICY	0..*	REQUEST_CRITERIA
4	0..1	ACCESS_POLICY	1..*	ATTESTATION_INFO

7.2.2 Target

Term: *target*

Definition: Specification of the parts of the EHR data to which this policy applies

Class name: TARGET

Description: This class specifies the parts of the EHR to which this policy applies. These parts might be specified as a profile (or filter) on the EHR, which might be expressed in terms of the rc_id of one particular FOLDER or a list of particular RECORD_COMPONENTS, and/or a set of archetypes, and/or a time period. Other selection criteria may also be included, as constraints expressed as strings. More than one profile might apply, and so the ACCESS_POLICY class may contain zero to many instances of TARGET. If no instances are specified this access policy applies to the whole EHR.

Attributes

#	Attribute name	Datatype	Description
1	rc_ids	II[0..*]	If this property is specified, this policy shall apply to all RECORD_COMPONENT instances corresponding with a member of the specified set.
2	archetype_id	II[0..*]	If this property is specified, this policy shall apply to all RECORD_COMPONENT instances conforming to any of the archetypes identified within this set.
3	time_period_start	TS[0..1]	If this property is specified, this policy shall apply to all RECORD_COMPONENT instances whose auditEvent-TimeStamp is at or after the date and time specified.
4	time_period_end	TS[0..1]	If this property is specified, this policy shall apply to all RECORD_COMPONENT instances whose auditEvent-TimeStamp is at or before the date and time specified.
8	other_criterion	String [0..*]	This property may be used to define any other computable or human readable inclusion or excision criterion that define the content of an EHR_EXTRACT to which this policy applies.

Relationships

#	Class name		Aggregation of	
1	1	ACCESS_POLICY	0..*	TARGET

7.2.3 Request criterion

Term: *request criterion*

Definition: Profile of the kind of EHR data processing request to which this policy applies.

Class name: REQUEST_CRITERIA

Description: This class specifies the kind of request profile to which this policy applies. The request profile (or scenario) can be specified in terms of a particular pattern of Functional Role, Structural role, Clinical setting, Specialty, Purpose of use and/or may specify individual actors. More than one profile might apply, and so the ACCESS_POLICY class may contain zero to many instances of REQUEST_CRITERIA. If no instances are specified this access policy applies to all possible request profiles.

Attributes

#	Attribute name	Datatype	Description
1	functional_role	CV[0..1]	If this property is specified, the processing functions permitted via the properties in the class SENSITIVITY_CONSTRAINTS only apply to a requesting party acting with this functional role. The default terminology for this property shall be as defined for functional role in ISO 21298, mirrored in 6.2 of this document, but jurisdictions may nominate or define other term lists as needed to comply with applicable legislation and requirements, as part of Normal Conformance to this document.
2	structural_role	CV[0..1]	If this property is specified, the processing functions permitted via the properties in the class SENSITIVITY_CONSTRAINTS only apply to a requesting party acting with this structural role. The default terminology for this property shall be as defined for structural role in ISO 21298, but jurisdictions may nominate or define other term lists as needed to comply with applicable legislation and requirements.
3	purpose	CV[0..1]	If this property is specified, the processing functions permitted via the properties in the class SENSITIVITY_CONSTRAINTS only apply to a requesting party acting with this purpose. The default terminology for this property shall be as defined in ISO TS 14265, but jurisdictions may nominate or define other term lists as needed to comply with applicable legislation and requirements.
4	clinical_setting	CV[0..1]	If this property is specified, the processing functions permitted via the properties in the class SENSITIVITY_CONSTRAINTS only apply to a requesting party acting within this care setting. No default term list is provided for this property.
5	speciality	CV[0..1]	If this property is specified, the processing functions permitted via the properties in the class SENSITIVITY_CONSTRAINTS only apply to a requesting party acting within this health or care speciality. The default terminology for this property shall be as defined in ISO TS 21298, but jurisdictions may nominate or define other term lists as needed to comply with applicable legislation and requirements.
6	party	II[0..1]	If this property is specified, the processing functions permitted via the properties in the class SENSITIVITY_CONSTRAINTS only apply to a requesting party specified through an instance of DEMOGRAPHIC_ENTITY with this identifier.
7	other_characteristic	String [0..1]	This property may be used to define any other computable or human readable characteristic of a requesting party to which this policy applies.

Relationships

#	Class name		Aggregation of	
1	1	ACCESS_POLICY	0..*	REQUEST_CRITERIA

7.2.4 Sensitivity constraint

Term: *sensitivity constraint*

Definition: Specification of the permissions that apply to requests matching the REQUEST_CRITERIA for EHR data that matches the TARGET specification

Class name: SENSITIVITY_CONSTRAINTS

Description: For minimum conformance to this document, the properties of this class are used to represent the applicable values from Table 1. Up to four values from Table 1 may be included for minimum conformance to this document, to represent the maximum sensitivity value that permits each of the four types of processing specified (access, write, modify, communicate). An additional property may be used to specify if the permitted processing applies to all versions of the EHR data or only to the most recent version. For normal conformance to this document, the policy rules shall be specified using the other_constraint property.

Attributes

#	Attribute name	Datatype	Description
1	access	Integer[0..1]	According to this policy requests for access to RECORD_COMPONENTS specified through properties of the TARGET class should be granted to parties specified according to properties of the REQUEST_CRITERIA class if the sensitivity of the RECORD_COMPONENTS is less than or equal to the value of this property.
2	write	Integer[0..1]	According to this policy the privilege to create new RECORD_COMPONENTS with a content profile specified through properties of the TARGET class should be granted to parties specified according to properties of the REQUEST_CRITERIA class if the sensitivity of the new RECORD_COMPONENTS is less than or equal to the value of this property.
3	modify	Integer[0..1]	According to this policy parties specified according to properties of the REQUEST_CRITERIA class may revise RECORD_COMPONENTS specified through properties of the TARGET class if the sensitivity of those RECORD_COMPONENTS is less than or equal to the value of this property.
4	communicate	Integer[0..1]	According to this policy parties specified according to properties of the REQUEST_CRITERIA class may onward-communicate RECORD_COMPONENTS specified through properties of the TARGET class if the sensitivity of those RECORD_COMPONENTS is less than or equal to the value of this property.
5	version_history	Boolean[1]	If this property value is true the policy authorises the permitted processing to include all versions of each RECORD_COMPONENT. If false processing is only authorised for only the most recent version of each included RECORD_COMPONENT.
6	other_constraints	String[0..*]	This property may be used to define any other computable or human readable processing privileges of the parties profiled through the requester, for the content of an EHR_EXTRACT to which this policy applies.

Relationships

#	Class name		Aggregation of	
1	1	ACCESS_POLICY	1	SENSITIVITY_CONSTRAINTS

7.2.5 Attestation information

Term: *attestation information*

Definition: *base component* documenting the details of an attestation of a set of *electronic health record components*

Class name: ATTESTATION_INFO

Description: See ISO 13606-1 for the documentation of this class.

The demographic extract to be included in an EHR audit log extract, shall include the information needed to identify all healthcare actors that are referenced from the EHR audit log extract.

Relationships

#	Class name		Aggregation of	
1	0..1	ACCESS_POLICY	1..*	ATTESTATION_INFO

7.3 Archetype of the access policy COMPOSITION

In order to enable access policy information to be included as part of an EHR_EXTRACT using the RECORD_COMPONENT hierarchy, a COMPOSITION Reference Archetype is defined in ISO 13606-3. The communication of access policy information using a COMPOSITION conforming to that Reference Archetype is a method for meeting normal conformance to this document.

8 Representing audit log information

8.1 General

This clause defines an information model for communicating an extract derived from the audit log of an EHR system that describes information that has been extracted and communicated from that system. It is not intended to be a computer security (forensic quality) audit log extract, but rather a way of communicating to a subject of care, or other appropriate parties, information about who has accessed that person's electronic health record.

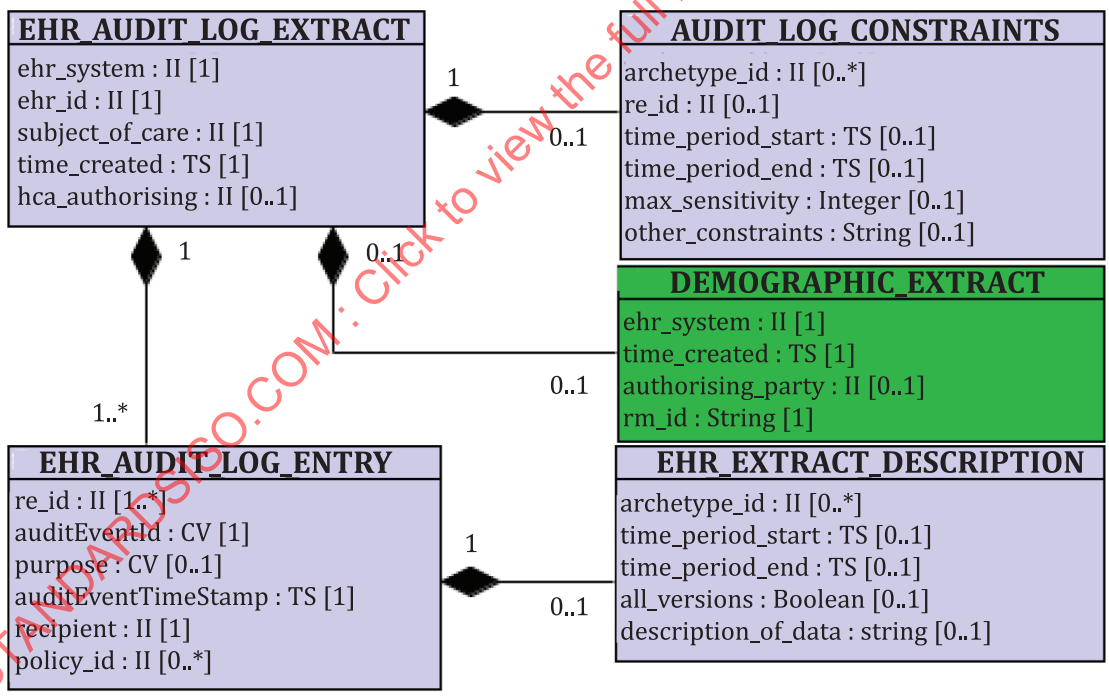


Figure 6 — UML model of the EHR Audit Log Extract

Figure 6 shows the information model to be used to communicate an extract of an EHR access log specifically intended to inform a patient about who has accessed his or her health record. An explanation of the classes and attributes is given below, together with the corresponding property in ISO 27789 where applicable.

8.1.1 EHR audit log extract

Term: *EHR audit log extract*

Definition: EHR audit log extracted from an EHR for the purpose of communication

Class name: EHR_AUDIT_LOG_EXTRACT

Description: This is the root class containing the information that has been extracted from an audit log, and is being communicated to a requester of this extract, in response to the REQUEST_EHR_AUDIT_LOG_EXTRACT interface defined according to ISO 13606-5. This class defines the EHR system from which the extract has been taken, the subject of care whose record it is an audit log from, and properties about the creation of this audit log extract.

Attributes

#	Attribute name	Datatype	Description
1	ehr_system	II[1]	Unique identifier of the EHR system from which the EHR has been accessed. Correspondence with ISO 27789: Audit enterprise site ID. (Logical source location within the healthcare enterprise network; for example, a hospital or other provider location within a multi-entity provider group.)
2	ehr_id	II[1]	Unique identifier of the electronic health record that has been accessed. Correspondence with ISO 27789: none.
3	subject_of_care	II[1]	Unique identifier for the subject of care to whom the EHR relates. Correspondence with ISO 27789: none.
4	time_created	TS[1]	Date and time that this audit log information was extracted from the audit log system. Correspondence with ISO 27789: EventDateTime.
5	hca_authorising	II[0..1]	Identifier of the healthcare actor who has authorized the creation and communication of this audit log extract. Correspondence with ISO 27789: none.

Relationships

#	Class name		Aggregation of	
1	1	EHR_AUDIT_LOG_EXTRACT	1..*	EHR_AUDIT_LOG_ENTRY
2	1	EHR_AUDIT_LOG_EXTRACT	0..1	AUDIT_LOG_CONSTRAINTS
3	0..1	EHR_AUDIT_LOG_EXTRACT	0..1	DEMOGRAPHIC_EXTRACT

8.1.2 Audit log constraint

Term: *Audit log constraint*

Definition: filter to be applied on the complete historic audit log when generating an EHR audit log extract for a specific purpose

Class name: AUDIT_LOG_CONSTRAINTS

Description: This class profiles the filter on the complete historic audit log that has been used to derive this extract. For example, it might be the part of an audit log within a specified date time period, and/or it might only contain information about access to certain kinds of health information (specified through one or more archetypes), and/or it might only report the audit log information for one or more precisely specified parts of the EHR (for example, a specific COMPOSITION, identified via its rc_id), and/or it might only contain disclosures made of RECORD_COMPONENTS of a particular sensitivity. These properties may be combined to define a very precise filter on the audit log extract that has been requested and provided.

Attributes

#	Attribute name	Datatype	Description
1	archetype_id	II [0..*]	Set of archetypes to which this audit log extract is limited. Correspondence with ISO 27789: none.
2	rc_id	II [0..*]	Set of RECORD_COMPONENTS to which this audit log extract is limited. Correspondence with ISO 27789: none.
3	time_period_start	TS [0..1]	The starting date and time which this audit log extract covers. Correspondence with ISO 27789: none.
4	time_period_end	TS [0..1]	The end date and time which this audit log extract covers. Correspondence with ISO 27789: none.
5	max_sensitivity	Integer [0..1]	Maximum sensitivity of RECORD_COMPONENT whose access is described in this audit log extract. Correspondence with ISO 27789: none.
6	other_constraints	String [0..1]	Any other constraints limiting the scope of this audit log extract. As this is a TEXT data type the specifications of additional constraints might not be suitable for automated processing. Correspondence with ISO 27789: none.

Relationships

#	Class name		Aggregation of	
1	1	EHR_AUDIT_LOG_EXTRACT	0..1	AUDIT_LOG_CONSTRAINTS

8.1.3 EHR audit log entry

Term: *EHR audit log entry*

Definition: part of an EHR audit log containing information about one single audit event

Class name: EHR_AUDIT_LOG_ENTRY

Description: This class represents one or more audit log entries that correspond to the filter requests, and provides a set of descriptors of the EHR information that was provided, or refused. It cannot be assumed that a party requesting an EHR audit log extract would automatically have rights to access the actual EHR content relating to this entry.

This class therefore only provides the set rc_id identifiers that would permit retrieval of the actual EHR content in question. However, such a retrieval would be actioned through a request for an EHR_EXTRACT, in accordance with ISO 13606-1 and ISO 13606-5, and be subject to appropriate access controls. The descriptors provided by this class include the purpose of use for which the EHR data were requested, when the data were provided and to whom, or if the request was declined. Other information about the handling of the response may also be included.

An EHR audit log extract contains a set of EHR audit log entries, each of which relates to one interaction with this EHR within this EHR system. An EHR audit log entry contains information about the EHR data that was accessed, to whom, and when.

Correspondence with ISO 27789: Note that the events provided through this EHR audit log extract should correspond to EHR audit log entries conforming to ISO 27789 for which the Audit Event Action Code has the value “R” (Read/View/Print/Query - Display or print data, such as a diagnosis).

Attributes

#	Attribute name	Datatype	Description
1	rc_id	II [1..*]	The set of RECORD_COMPONENTS included in the EHR_EXTRACT. Correspondence with ISO 27789: none.
2	auditEventId	CV[1]	This property mirrors a property of the AUDIT_INFO class in ISO 13606-1. Correspondence with ISO 27789: Event ID. (Unique identifier for the specific audited event).
3	purpose	CV [0..1]	Description of the rationale for the EHR request. The values for this property shall be one of the category codes defined for purposes of use in ISO TS 14265. Correspondence with ISO 27789: Purpose of use (which also refers to ISO TS 14265 for its term list).
4	auditEventTimestamp	TS[1]	Date and time when the EHR system provided its response. Correspondence with ISO 27789: Event date and time (A date/time specification that is unambiguous as to local time zones).
5	recipient	II[1]	Healthcare actor to whom the EHR data was communicated. This might or might not be the person specified as recipient in the request. Correspondence with ISO 27789: UserID (Unique identifier for the user actively participating in the event.)
6	policy_id	II [0..*]	Reference to one or more policies that were applied to the access decision reflected in this audit log entry. Correspondence with ISO 27789: Participant Object Policy Permission Set. (Pointer to the policies that cover and access to the Participant Object ID).

Relationships

#	Class name		Aggregation of	
1	1	EHR_AUDIT_LOG_ENTRY	0..1	EHR_EXTRACT_DESCRIPTION
2	1	EHR_AUDIT_LOG_EXTRACT	1..*	EHR_AUDIT_LOG_ENTRY

8.1.4 EHR extract description

Term: *EHR extract description*

Definition: set of descriptors that summarise the kind of information that was provided in an EHR extract

Class name: EHR_EXTRACT_DESCRIPTION

Description: This class represents the set of descriptors that summarise the kind of information that was provided in the EHR extract that an EHR audit log entry relates to. The disclosed EHR data are described through listing the archetype_ids, the time period covered by the extract if it was itself derived through a time filter, and if only the latest version or if all versions of the data were disclosed. These descriptors are intended to provide sufficient information to explain the nature of disclosures that have occurred without providing the actual EHR data content.

Attributes

#	Attribute name	Datatype	Description
1	archetype_id	II [0..*]	Archetypes included in the EHR_EXTRACT. Correspondence with ISO 27789: none.
2	time_period_start	TS [0..1]	Starting date and time covered by the EHR_EXTRACT, if it was derived as a time period filter of the EHR. Correspondence with ISO 27789: none.
3	time_period_end	TS [0..1]	Final date and time covered by the EHR_EXTRACT, if it was derived as a time period filter of the EHR. Correspondence with ISO 27789: none.
4	all_versions	Boolean [0..1]	If all versions were included in the EHR_EXTRACT. Correspondence with ISO 27789: none.
5	description_of_data	String [0..1]	Any other details that describe the EHR_EXTRACT or constraints applied to its creation. Correspondence with ISO 27789: Participant object detail.

Relationships

#	Class name		Aggregation of	
1	1	EHR_AUDIT_LOG_ENTRY	0..1	EHR_EXTRACT_DESCRIPTION

8.1.5 Demographic extract

Term: *Demographic extract*

Definition: demographic information extracted for the purpose of being included in an *EHR extract* or an *EHR audit log extract*

Class name: DEMOGRAPHIC_EXTRACT

Description: See ISO 13606-1 for the documentation of this class.

Because the recipient of the EHR_EXTRACT is only defined in the class EHR_AUDIT_LOG_ENTRY via an identifier, the class DEMOGRAPHIC_EXTRACT provides the descriptive information (such as name, organisation, specialty) of the recipients included within this audit log extract.

Correspondence with ISO 27789: none.

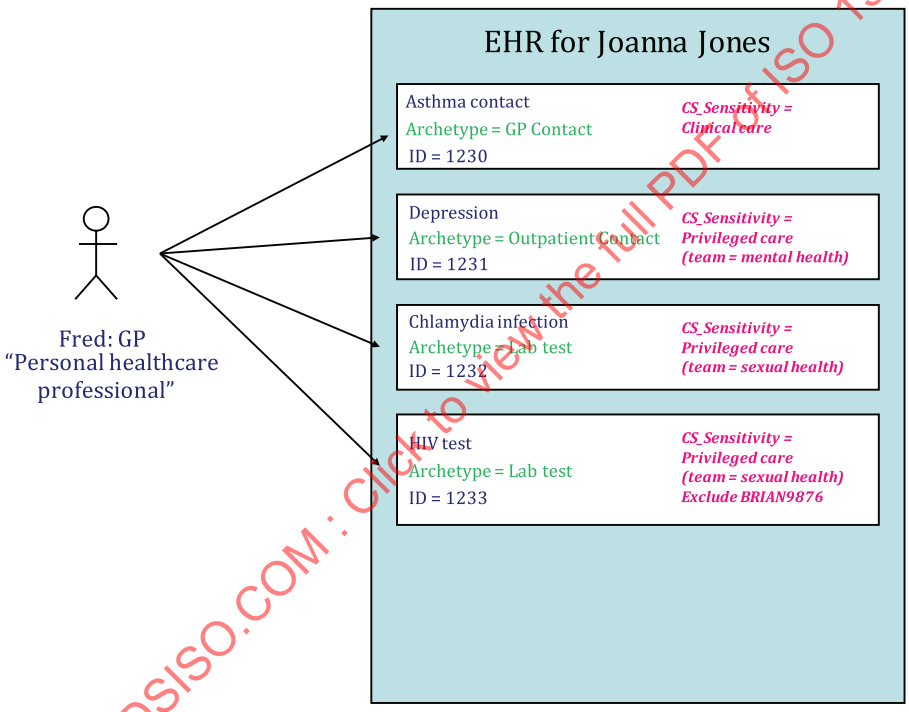
#	Class name		Aggregation of	
1	0..1	EHR_AUDIT_LOG_EXTRACT	0..1	DEMOGRAPHIC_EXTRACT

Annex A
(informative)

Illustrative access control example

The diagrams below provide an illustration of the way in which comparatively simple policies can offer quite a flexible way of managing access to the data within one EHR.

In this example, Joanna Jones has four Compositions in her EHR: an Asthma contact with her GP, an outpatient (ambulatory care) consultation for depression with a psychiatrist, a laboratory test performed in a sexual health clinic confirming the presence of a Chlamydia infection, and an HIV test result. Each of these has a defined sensitivity (in accordance with 6.1 of this document). The HIV test also references a policy by which a named party is denied access to this Composition.



Fred is Joanna's General Practitioner; he is able to access her EHR in the Functional Role of Personal Clinician. He is able to access all four of these Compositions.