TECHNICAL SPECIFICATION

ISO/TS 13606-4

First edition
2009-10-01

Health informatics — Electronic health record communication —

Part 4: Security

Informatique de santé — Communication du dossier de santé informatisé —

Partie 4: Sécurité

Reference number
ISO/TS 13606-4:2009(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

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

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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

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

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

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

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

— *Part 1: Reference model*

— *Part 2: Archetype interchange specification*

— *Part 3: Reference archetypes and term lists*

— *Part 4: Security* [Technical Specification]

— *Part 5: Interface specification*

0 Introduction

0.1 Challenge addressed by this part of ISO 13606

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

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

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

— numbers of health record entries made on a patient during the course of modern healthcare;

— numbers of healthcare personnel, often rotating through posts, who might potentially come into contact with a patient at any one time;

— numbers of organizations with which a patient might come into contact during his or her lifetime;

— difficulty (for a patient or for anyone else) of classifying, in a standardized way, how sensitive a record entry might be;

— difficulty of determining how important a single health record entry might be to the future care of a patient and to which classes of user;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

0.2 Communication scenarios

0.2.1 Data flows

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

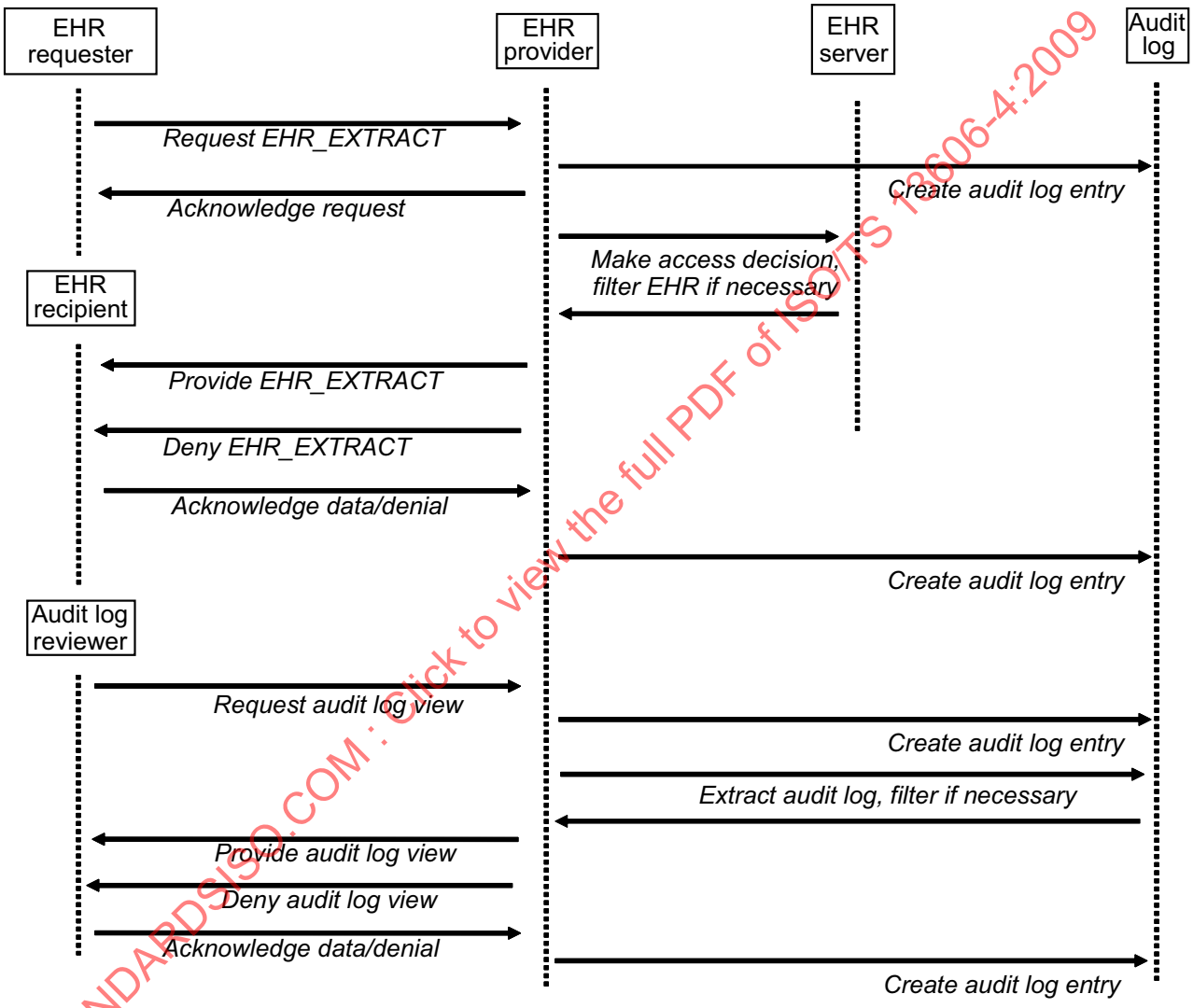


Figure 1 — Principal data flows and security-related business processes covered by this part of ISO 13606

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

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

0.2.2 Request EHR data

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

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

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

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

0.2.3 Generate EHR access log entry

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

0.2.4 Acknowledge receipt of EHR_Request

No healthcare-specific security considerations.

0.2.5 Make access decision, filter EHR data

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

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

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

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

0.2.6 Deny EHR_EXTRACT

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

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

0.2.7 Provide EHR_EXTRACT

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

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

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

0.2.8 Acknowledge receipt of EHR_EXTRACT

No healthcare-specific security considerations.

0.2.9 Generate EHR access log entry

(As 0.2.3)

0.2.10 Request EHR access log view

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

The interface model is defined in ISO 13606-5.

0.2.11 Generate EHR access log entry

(As 0.2.3)

0.2.12 Provide EHR access log view

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

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

The interface model is defined in ISO 13606-5.

0.2.13 Deny EHR access log view

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

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

0.2.14 Acknowledge receipt of EHR access log view

No healthcare-specific security considerations.

0.2.15 Generate EHR access log entry

(As 0.2.3)

0.3 Requirements and technical approach

0.3.1 Research on the requirements

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

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

— authorization, privilege and access control management;

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

— security classification of EHR information;

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

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

— overall safety and quality procedures.

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

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

0.3.2 Generic healthcare security requirements

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

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

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

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

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

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

0.3.3 Generic healthcare access control architecture

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

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

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

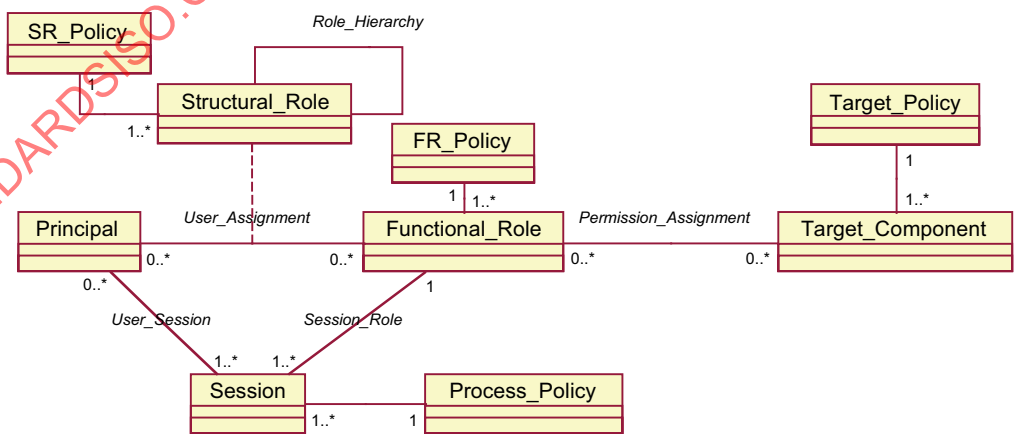


Figure 2 — Main concepts and policy types defined in role based access control

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

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

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

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

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

0.3.4 Security requirements specific to EHR communications

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

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

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

0.4 Generic EHR access policy model

0.4.1 Factors considered when defining EHR access policies

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

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

---

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

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

User characteristics:

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

Access characteristics:

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

Organizational policies might also confirm permissions about:

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

EHR-specific policies might provide or deny consent for:

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

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

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

d) specific purposes for the access;

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

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

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

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

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

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

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

0.4.2 EHR access policies: a minimum specification for interoperability

0.4.2.1 General

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

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

These two vocabularies are:

1) sensitivity classification of EHR data (RECORD_COMPONENTS);

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

0.4.2.2 Defining "need-to-know" when handling EHR data

Within a clinical care environment (i.e. 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.

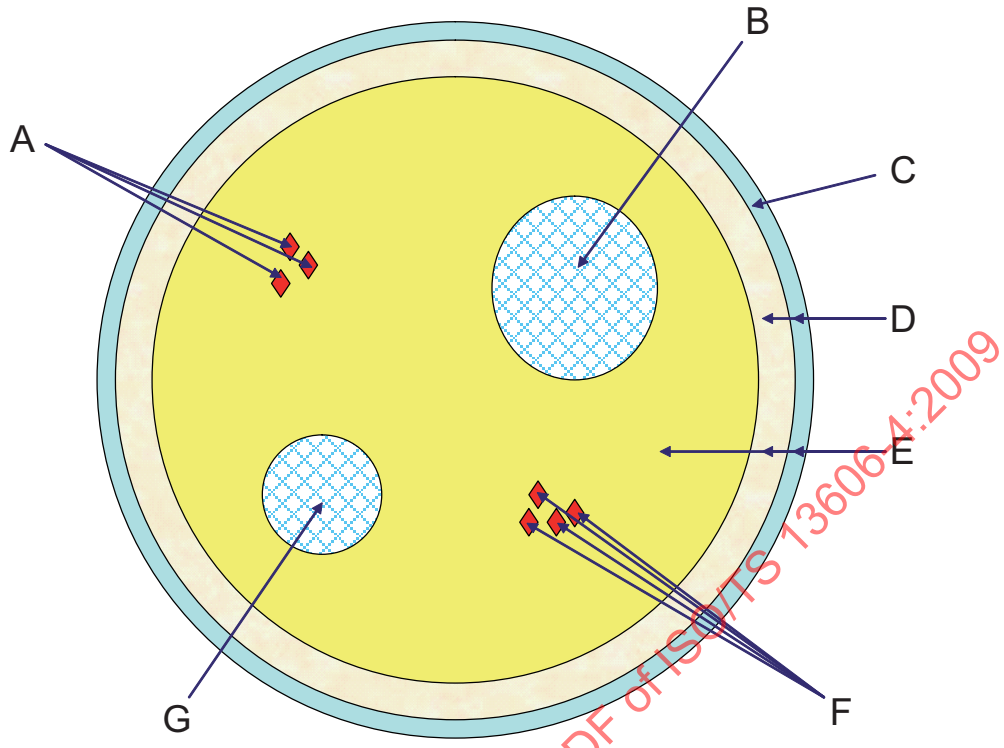
Few contemporary healthcare systems (on paper or electronically) define complex internal access control partitions to the health records that they hold. Even if it were considered useful to define numerous fine-grained access policies, in practice it might take healthcare systems, national health services 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 rights 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 organizations, and is not the scope of this part of ISO 13606.) However, it is also well accepted that patients and professionals may 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.

ISO 27799 draws attention to the challenges of defining how sensitive particular items of personal health information might be. That this is often judged subjectively by data subjects depending upon their personal situation, which might change over time, and also by the care setting in which data were acquired or might be accessed. ISO 27799 recognises the need for, and advocates, the classification and labelling of assets such as personal information, in order to indicate need-to-know.

Figure 3 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	E	entries accessible to direct care teams
B	entries restricted to sexual health team	F	private entries shared with several named parties
C	entries accessible to administrative staff	G	entries restricted to prison health services
D	entries accessible to clinical support staff		

Figure 3 — Illustration of access domains within an example EHR

In Figure 3, 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 may nominate other parties to access these subsets of the EHR if he or she wishes.) One aspect of privilege is the assignment by an organization of roles to a clinician, which may be exercised in an emergency that confer rights 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 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 may 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. Appointment 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 6, 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 patient, 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 (Annex A), this part of ISO 13606 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 RECORD_COMPONENTs within it according to the classification defined in 5.1. This classification corresponds to the various sub-domains of EHR data illustrated in Figure 3.

In practice any given EHR system might have other mechanisms for indicating the sensitivity of EHR data or some equivalent concept. This part of ISO 13606 does not require EHR systems to store data according to the sensitivity levels defined in 5.1, but to be able to map to this classification on generating an EHR_EXTRACT.

0.4.2.3 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 part of ISO 13606 does require 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 5.2.

This set of functional roles is identical to that proposed to be included in ISO/TS 21298. It is included here as a normative specification.

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 5.3.

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 may 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 may be combined with a small number of additional specifications to specify a relatively rich set of access constraints is provided in Clause 6.

0.5 Audit log interoperability

It is widely recognised that the details of interactions with an EHR system are required to be retained for auditability purposes. However, the way in which these kinds of audit log are implemented is quite specific for each EHR system, partly determined by the persistence (e.g. database storage) approach adopted, and might also partly be directed by local or national legislation. Formal standards for audit log interoperability and communication are not yet available.

Requirements for interoperable audit logs will be specified in ISO 27789, which is currently under development. ISO 27789 will define trigger events and data elements for EHR audit log entries. [A specification for representing audit logs was also published in 2004 as an informational draft by IETF (RFC 3881).]

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. This is therefore defined both as an audit log review information model in Clause 7 and as a request and response interface model in ISO 13606-5.

It is recognised that so few systems today could meet this requirement that conformance to this provision is considered separately from conformance to the rest of this part of ISO 13606. It is therefore a matter of local or national policy to dictate if this additional provision is to be met.

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. This Technical Specification does not define any interoperable specifications for such examinations.

0.6 Relationship to ENV 13606-3

The distribution rules of ENV 13606, published in 2000, provided a detailed analytical framework for specifying requirements that are to be met in order to sanction the communication of EHR data. Experience fed back to the present EHRcom task force team is that this framework, although very rich, was difficult to implement in practice for several reasons:

- some aspects of the specification, such as the Why (the purpose for which an EHR communication was requested) are defined with textual attributes without a formalized vocabulary, making interoperability difficult to achieve;
- overall framework was far more detailed than the access control provisions of most contemporary EHR systems, and would be both costly and difficult to implement;
- framework would require significant operational effort from healthcare professionals, to populate rule instances during EHR data entry;
- many computerized health systems were and are incorporating generic security measures, and the addition of an EHR-specific approach was felt to be unnecessary.

Since 2000 many health services have developed strategies for securing healthcare systems and communications between them, and many products now incorporate or interface with generic security components such as certificate services and PKI systems. Security standards published since 2000 now address many of the aspects that were then necessary to specify in the distribution rules.

The approach taken in this part of ISO 13606 is to advocate the use of these industry standards or health domain (generic) security measures, and to specify only those features that pertain to EHR communications in particular – most notably the access provisions that might be specifically associated with any given electronic health record. The most common example of this will be the disclosure wishes of the patient (the data subject).

A more detailed description of these changes is given in Annex B.

Health informatics — Electronic health record communication —

Part 4: Security

1 Scope

This part of ISO 13606 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 part of ISO 13606 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 part of ISO 13606.

2 Conformance

This part of ISO 13606 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, which 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 5.1. 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 5.2. 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 5.3.

For “normal conformance”, the EHR_EXTRACT shall contain or reference a generic representation of any policy information relating to the EHR data being communicated, either explicitly according to 6.3, or logically according to 6.4 in conjunction with another published standard for access policy representation. 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.

For “extended conformance”, if an interoperable audit log view is required, in addition to normal conformance, the information model in Clause 7 shall be used to represent that view.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
access control
a means of ensuring that resources of data processing systems can only be accessed through authorized channels by authorized entities

NOTE Adapted from ISO/IEC 2382-8:1998.

3.2
access policy
process that defines obligations for authorizing access control to a resource

3.3
auditability
property that ensures that any action of any security subject on any security object may be examined in order to establish the real operational responsibilities

[ENV 13608-1:2000]

3.4
authentication
process of reliably identifying security subjects by securely associating an identifier and authenticator

3.5
authorization
granting of rights

3.6
authority
entity responsible for issuing certificates

3.7
availability
property of being accessible and useable upon demand by an authorized entity

[ISO 7498-2:1989, definition 3.3.11]

3.8
confidentiality
process that ensures that information is accessible only to those authorized to have access

3.9
EHR extract
healthcare subject's partial or full electronic health record, communicated so that it complies with this part of ISO 13606

3.10
EHR provider
entity in legitimate possession of EHR data and in a position to communicate it to another appropriate entity

3.11
EHR recipient
entity to whom EHR data is communicated by an EHR provider

3.12
EHR requester
entity initiating a request for EHR communication to take place between an EHR provider and an EHR recipient

3.13
identification
identity authentication
identity validation
performance of tests to enable a data processing system to recognise entities

[ISO/IEC 2382-8:1998, definition 08.04.12]

3.14
identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

[ENV 13608-1:2000]

3.15
key
sequence of symbols which controls the operations of encipherment and decipherment

[ISO 7498-2:1989, definition 3.3.32]

3.16
policy
set of legal, political, organizational, functional and technical obligations for communication and cooperation

[ISO/TS 22600-1:2006, definition 2.13]

3.17
privilege
capacity assigned to an entity by an authority

3.18
public key infrastructure
PKI
infrastructure used in the relation between a key holder and a relying party which allows a relying party to use a certificate relating to the key holder for at least one application using a public key dependent security service and which includes a certification authority, a certificate data structure, means for the relying party to obtain current information on the revocation status of the certificate, a certification policy and methods to validate the certification practice

[ISO 17090-1:2008, definition 3.3.18]

3.19
role
set of competences and/or performances associated with a task

3.20
sensitivity
measure of importance assigned to information to denote its need for protection

3.21
security
combination of availability, confidentiality, integrity and accountability

[ENV 13608-1:2000]

3.22
security policy
plan or course of action adopted for providing computer security

[ISO/IEC 2382-8:1998, definition 08.01.06]

3.23
security service
service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers

[ISO 7498-2:1989, definition 3.3.51]

3.24
subject of care
person seeking to receive, receiving or having received healthcare

NOTE Adapted from EN 14822-2:2005.

3.25
target
resource being accessed

4 Abbreviations

— ADL archetype definition language

— EHR electronic health record

— EHRA electronic health record architecture

— PKI public key infrastructure

— PMAC privilege management and access control

— UML unified modelling language

5 Record component sensitivity and functional roles

5.1 RECORD_COMPONENT sensitivity

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

Table 2 — Values of CS_SENSITIVITY to be used for the sensitivity attribute of RECORD_COMPONENT

CS_SENSITIVITY value	Sensitivity level	Description of intended access to RECORD_COMPONENTs 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, e.g. mental health)
Clinical care	3	Default for normal clinical care access (i.e. most clinical staff directly caring for the patient should be able to access nearly all of the EHR)
Clinical management	2	Less sensitive RECORD_COMPONENTs, that might need to be accessed by a wider range of personnel not all of whom are actively caring for the patient (e.g. radiology staff)
Care management	1	RECORD_COMPONENTs that might need to be accessed by a wide range of administrative staff to manage the subject of care's access to health services

5.2 Functional roles

The functional role of any intended EHR recipient shall be one of the values for functional role defined in Table 3. The roles defined here are aligned with the functional roles defined in ISO/TS 21298.

Table 3 — List of functional roles

Functional role	Brief description
Subject of care	Principal data subject of the electronic health record
Subject of care agent	For example, parent, guardian, carer or other legal representative
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)
Healthcare professional	Party involved in providing direct care to the patient
Health-related professional	Party indirectly involved in patient care, teaching, research, etc.
Administrator	Any other parties supporting service provision to the patient

5.3 Mapping of functional role to RECORD_COMPONENT sensitivity

When making an access decision, at a minimum, Table 4 shall be used to determine the sensitivities of RECORD_COMPONENT to which an EHR recipient may be granted access according to the functional role defined in the EHR request.

Table 4 — Mapping of functional roles to RECORD_COMPONENT sensitivity

Functional role	RECORD_COMPONENT sensitivity				
	Care management	Clinical management	Clinical care	Privileged care	Personal care
Subject of care	Y	Y	Y	Y	Y
Subject of care agent	Y	Y	Y	Y	Y
Personal healthcare professional	Y	Y	Y	Y	Y
Privileged healthcare professional	Y	Y	Y	Y+	++
Healthcare professional	Y	Y	Y	—	—
Health-related professional	Y	Y	—	—	—
Administrator	Y	—	—	—	—

Y Indicates that access will be granted to RECORD_COMPONENTs of this sensitivity unless otherwise dictated by other policy constraints, as specified according to Clause 7.

\+ 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 RECORD_COMPONENT was created, e.g. sexual health clinic, prison health service [as specified in the service_setting attribute for the composer of the COMPOSITION in the reference model (ISO 13606-1)]. This access may also be granted in healthcare emergency situations if so authorized.

++ Indicates that access to personal care information may sometimes be granted by mandate to privileged healthcare professionals in some care settings, such as in the armed forces of some countries.

6 Representing access policy information within an EHR_EXTRACT

6.1 General

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 to access the EHR data.

NOTE COMPOSITIONS can be attested, and proof of that attestation included, within the EHR_EXTRACT.

The entire FOLDER is optional, as it may 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 the specification in 6.3. Each instance 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.

This part of ISO 13606 has adopted the approach of representing policy information as COMPOSITIONS conforming to ISO 13606-1, rather than defining a separate information model, 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 RECORD_COMPONENTS within an EHR_EXTRACT. It is therefore possible, for example, to include or reference the signature of the patient 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 6.4, may instead be represented and communicated as an ISO 22221

(PMAC) policy, in situations where the communicating parties share a common consent and authorization architecture.

The access policy COMPOSITION archetype comprises three SECTIONS and one additional ENTRY to represent the effective time of the policy, when it is to be enforced. The effective time is an interval, whose start or end time may be nil to indicate an immediate start and/or an indefinite duration.

The request specification SECTION is used to define the kind of request scenario to which this policy applies. The kind of request may be specified in terms of particular functional roles (as specified in Clause 5), functional responsibilities (which are like locally-defined functional roles), structural roles, clinical settings or specialities. Individual parties (e.g. persons, organizations, devices, agents) may be identified, through an instance identifier that may be mapped to a fuller description of the party in the DEMOGRAPHIC_EXTRACT (as defined in ISO 13606-1). Any other characteristics needed to define the request may be specified as a list of strings. Each of these ways of defining the request scenario is represented as a list of one or more ELEMENTS within a containing ENTRY.

The list of ELEMENTS within an ENTRY form a union set. The set of ENTRIES within the SECTION form an intersection set. This request specification may therefore be used, for example, to indicate that the policy applies to requests to provide EHR data to psychiatrists or to gynaecologists working at a specified hospital.

The EHR_target SECTION is used to define the parts of the patient's EHR to which the policy applies. The parts of the EHR may 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 may 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 the request specification, the list of ELEMENTS within an ENTRY form a union set and the set of ENTRIES within the EHR_target SECTION form an intersection set.

The access rules SECTION is used to define the permissions that apply to requests matching the request specification for data that matches the EHR_target specification. At its simplest level, the rule might be to permit or deny full access to the target data. However, to offer some flexibility, the maximum sensitivity 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 2. 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 maximum sensitivity 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 rights 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 access rules SECTION 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 may be specified as strings. If other string specifications are used, 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 should be satisfied that the EHR recipient is able to understand and accommodate those additional rules.

Jurisdictions and EHR systems vary in the levels of granularity of the EHR hierarchy at which access controls are specified and implemented. Clearly, if controls are defined down to very fine grained levels (e.g. ENTRY or below) different classes of user might have very different views on the same COMPOSITION, creating clinical risk and a version management risk. Furthermore, if an EHR_EXTRACT specifies access controls at a lower level than in the importing system, it will be difficult for that importing system to effect the controls faithfully. A decision will need to be taken in such situations on whether to minimise clinical risk (e.g. by

applying to a whole COMPOSITION a policy equivalent to the least stringent controls of its content) or minimising legal risk (e.g. by applying to a whole COMPOSITION a policy that is equivalent to the most stringent control of its content). It is therefore suggested that jurisdictions encourage the application of policies to whole COMPOSITIONS or sets of COMPOSITIONS rather than to finer grained SECTIONS or ENTRIES wherever possible.

Note 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.

6.2 Archetype of the access policy COMPOSITION

Figure 4 shows the structure of the access policies archetype tree. Indentation to the right implies containment. Each class of RECORD_COMPONENT is shown using the following key (and colour, although the colours are not required in order to interpret the legend or figure):

— F: xxx in brown indicates a FOLDER with the meaning attribute value of xxx

— C: xxx in red indicates a COMPOSITION with the meaning attribute value of xxx

— S: xxx in orange indicates a SECTION with the meaning attribute value of xxx

— E: xxx in dark blue indicates an ENTRY with the meaning attribute value of xxx

— c: xxx in purple indicates a CLUSTER with the meaning attribute value of xxx

— e: xxx in green indicates an ELEMENT with the meaning attribute value of xxx

— D_V: XXXX indicates a Data Value with a data value type of XXXX

Optionality and cardinality for each node of the hierarchy are shown to the left of the node name.

EHR_EXTRACT							
0..1	**F: Access policies**						
	*0..**	**C: Access policy**					
		1..1	**E: Effective time**				
			*1..**	**e: time interval**			
					D_V: IVL<TS>		
		0..1	**S: Request specification**				
			0..1	**E: Functional roles**			
				*1..**	**e: functional role**		
						D_V: CS_FUNC_ROLE	
			0..1	**E: Functional responsibilities**			
				*1..**	**e: functional responsibility**		
						D_V: CV	
			0..1	**E: Structural roles**			
				*1..**	**e: structural role**		
						D_V: CV	
			0..1	**E: Clinical settings**			
				*1..**	**e: clincial setting**		
						D_V: CS_SETTING	
			0..1	**E: Specialities**			
				*1..**	**e: speciality**		
						D_V: CV	
			0..1	**E: Parties**			
				*1..**	**e: identified_party**		
						D_V: II	
			0..1	**E: Other requestor characteristics**			
				*1..**	**e: EHR requestor description**		
						D_V: TEXT	
		0..1	**S: EHR_target**				
			0..1	**E: Record components**			
				*1..**	**e: rc_id**		
						D_V: II	
			0..1	**E: Archetypes**			
				*1..**	**e: archetype_id**		
						D_V: II	
			0..1	**E: Time period**			
				*1..**	**e: time interval**		
						D_V: IVL<TS>	
			0..1	**E: Other selection criterion**			
				*1..**	**e: EHR selection criterion**		
						D_V: TEXT	
		1..1	**S: Access rules**				
			0..1	**E: Maximum sensitivity**			
				1..1	**e: access**		
						D_V: INT	
				1..1	**e: create**		
						D_V: INT	
				1..1	**e: revise**		
						D_V: INT	
				1..1	**e: communicate**		
						D_V: INT	
			1..1	**E: Version history**			
				1..1	**e: all_versions**		
						D_V: BL	
			*0..**	**E: Other rules**			
				*1..**	**e: access_rule**		
						D_V: TEXT	

Figure 4 — Diagrammatic representation of the access policy archetype

6.3 ADL representation of the archetype of the access policy COMPOSITION

This specification formally defines the access policies archetype, using the Archetype Definition Language (ADL) specified in ISO 13606-2. This is the formal expression of the model shown in Figure 4, and logically equivalent to the UML representation in Figure 5.

Conformance to this part of ISO 13606 requires that RECORD_COMPONENTS corresponding to this archetype and conforming to ISO 13606-1 are included within an EHR_EXTRACT in order to communicate access policy information within an EHR_EXTRACT. It does not require that ADL is itself used to represent or communicate this information. ADL is being used in this subclause as the formalism to specify the archetype within this part of ISO 13606.

```
archetype
    CEN-EN13606-COMPOSITION.access_policy.v1

concept
    [at0000]    -- Access policies for CEN EN13606 Extract

description
    original_author = <
        ["name"] = <"Dipak Kalra">
        ["organisation"] = <"www.chime.ucl.ac.uk">
    >
    other_contributors = <
        ["1"] = <"xxxx">
        ["2"] = <"xxxx">
    >
    lifecycle_state = <"draft">
    archetype_package_uri = <http://www.centc251.org/somewhere>
    details = <
        ["en"] = <
            language = <"en">
            purpose = <"To communicate the specific disclosure constraints that should
apply to Record Components contained within this EHR Extract">
            keywords = <"Access control", "security policy", "sensitivity", "privilege
management", "role based access control">
            use = <"This model is intended to communicate those constraints on access that
should apply to future access requests to information in this EHR Extract, usually those
that have been expressed by the subject of care">
            misuse = <"It is not intended to represent all of the policies that were used
to generate this EHR Extract: those policies have already been applied by the EHR provider
in creating the extract, and some of those might not be relevant to the EHR recipient">
            copyright = <"CEN">
            original_resource_uri = <
                ["xxx"] = <http://to_be_confirmed.later.org/xyz>
            >
        >
    >

definition
    COMPOSITION[at0000] matches {
        content cardinality matches {1..*} matches {
            ENTRY[at0001] occurrences matches {1..1} matches {
                data cardinality matches {1..*} matches {
                    ELEMENT[at0002] matches {
                        value matches {
                            IVL<TS> matches {*}
                        }
                    }
                }
            }
            SECTION[at0003] occurrences matches {0..1} matches {
                items cardinality matches {0..*} matches {
                    ENTRY[at0004] occurrences matches {1..1} matches {
                        data cardinality matches {1..*} matches {
                            ELEMENT[at0005] matches {
```

```
                value matches {
                    CS_FUNC_ROLE matches {*}
                }
            }
        }
    }
    ENTRY[at0006] occurrences matches {1..1} matches {
        data cardinality matches {1..*} matches {
            ELEMENT[at0007] matches {
                value matches {
                    CV matches {*}
                }
            }
        }
    }
    ENTRY[at0008] occurrences matches {1..1} matches {
        data cardinality matches {1..*} matches {
            ELEMENT[at0009] matches {
                value matches {
                    CS_SETTING matches {*}
                }
            }
        }
    }
    ENTRY[at0010] occurrences matches {1..1} matches {
        data cardinality matches {1..*} matches {
            ELEMENT[at0011] matches {
                value matches {
                    CV matches {*}
                }
            }
        }
    }
    ENTRY[at0012] occurrences matches {1..1} matches {
        data cardinality matches {1..*} matches {
            ELEMENT[at0013] matches {
                value matches {
                    II matches {*}
                }
            }
        }
    }
    ENTRY[at0014] occurrences matches {1..1} matches {
        data cardinality matches {1..*} matches {
            ELEMENT[at0015] matches {
                value matches {
                    TEXT matches {*}
                }
            }
        }
    }
  }
}
SECTION[at0016] occurrences matches {0..1} matches {
    items cardinality matches {0..*} matches {
        ENTRY[at0017] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0018] matches {
                    value matches {
                        CS_FUNC_ROLE matches {*}
                    }
                }
            }
        }
        ENTRY[at0019] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0020] matches {
                    value matches {
```

```
                        CV matches {*}
                    }
                }
            }
        }
        ENTRY[at0021] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0022] matches {
                    value matches {
                        CS_SETTING matches {*}
                    }
                }
            }
        }
        ENTRY[at0023] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0024] matches {
                    value matches {
                        CV matches {*}
                    }
                }
            }
        }
    }
}
SECTION[at0025] occurrences matches {1..1} matches {
    items cardinality matches {0..*} matches {
        ENTRY[at0026] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0027] matches {
                    value matches {
                        INT matches {*}
                    }
                }
                ELEMENT[at0028] matches {
                    value matches {
                        INT matches {*}
                    }
                }
                ELEMENT[at0029] matches {
                    value matches {
                        INT matches {*}
                    }
                }
                ELEMENT[at0030] matches {
                    value matches {
                        INT matches {*}
                    }
                }
            }
        }
        ENTRY[at0031] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0032] matches {
                    value matches {
                        BL matches {*}
                    }
                }
            }
        }
        ENTRY[at0033] occurrences matches {1..1} matches {
            data cardinality matches {1..*} matches {
                ELEMENT[at0034] matches {
                    value matches {
                        TEXT matches {*}
                    }
                }
            }
```

```
                    }
                }
            }
        }
    }

ontology
    primary_language = <"en">
    languages_available = <"en">
    term_definitions = <
        ["en"] = <
            items = <
                ["at0000"] = <
                    description = <"Access policies for CEN EN13606 Extract">
                    text = <"Access policies">
                >
                ["at0001"] = <
                    description = <"Time periods within which this policy is to be put into
effect">
                    text = <"effective time">
                >
                ["at0002"] = <
                    description = <"A specific time interval within which this policy is to
be put into effect">
                    text = <"time interval">
                >
                ["at0003"] = <
                    description = <"Set of  characteristics defining the kind of future EHR
request for which this policy is intended to be used ">
                    text = <"request specification">
                >
                ["at0004"] = <
                    description = <"The set of requester functional roles to which this
policy applies">
                    text = <"functional roles">
                >
                ["at0005"] = <
                    description = <"A functional role as defined in Section 6.2 of this
part-standard">
                    text = <"functional role">
                >
                ["at0006"] = <
                    description = <"The set of requester structural roles to which this
policy applies">
                    text = <"structural roles">
                >
                ["at0007"] = <
                    description = <"A structural role, in future to be taken from a set
defined by ISO TC/215">
                    text = <"structural role">
                >
                ["at0008"] = <
                    description = <"The set of requester clinical settings to which this
policy applies">
                    text = <"clinical settings">
                >
                ["at0009"] = <
                    description = <"A specific clinical setting, taken from a prescribed
list of clinical settings defined in Part 3 of this part standard">
                    text = <"clinical setting">
                >
                ["at0010"] = <
                    description = <"The set of requester clinical specialities to which
this policy applies">
                    text = <"specialities">
                >
                ["at0011"] = <
```

```
                description = <"Any coded representation of the clinical speciality to
which this policy applies: it will be for local policy to determine which term set must be
used to support interoperability">
                text = <"speciality">
            >
            ["at0012"] = <
                description = <"The set of individuals to whom this policy applies">
                text = <"parties">
            >
            ["at0013"] = <
                description = <"A specific identified party">
                text = <"identified party">
            >
            ["at0014"] = <
                description = <"A set of additional descriptors of the EHR Request,
which might be specified locally and/or required to comply with local or national policy
or legislation">
                text = <"other requestor characteristics">
            >
            ["at0015"] = <
                description = <"A specific descriptor of the requester profile to which
this policy applies">
                text = <"requestor description">
            >
            ["at0016"] = <
                description = <"Set of  characteristics defining the parts of the EHR
of this subject of care to which this policy is intended to be applied ">
                text = <"EHR target">
            >
            ["at0017"] = <
                description = <"A list of specific Record Component instances to which
the policy applies">
                text = <"record components">
            >
            ["at0018"] = <
                description = <"A particular Record Component to which this policy
applies">
                text = <"rc_id">
            >
            ["at0019"] = <
                description = <"A list of Archetypes to which the policy applies">
                text = <"archetypes">
            >
            ["at0020"] = <
                description = <"The identifier of an archetype: this policy applies to
all instances of Record Component conforming to part of this archetype">
                text = <"archetype_id">
            >
            ["at0021"] = <
                description = <"A set of time intervals: this policy applies to all
instances of Record Component committed within any of these time intervals">
                text = <"time period">
            >
            ["at0022"] = <
                description = <"A specific time interval: this policy applies to all
instances of Record Component committed within this time interval">
                text = <"time interval">
            >
            ["at0023"] = <
                description = <"A set of additional descriptors of part of this
subject's EHR to which this policy applies">
                text = <"other selection criterion">
            >
            ["at0024"] = <
                description = <" A specific descriptor of the Record Components to
which this policy applies">
                text = <"EHR selection criterion">
            >
```

```
                ["at0025"] = <
                    description = <"The set of permissions (rules) that this policy
dictates">
                    text = <"access rules">
                >
                ["at0026"] = <
                    description = <"The maximum level of Record Component sensitivity
granted by this policy to the profiled requestor in respect of the defined EHR target data,
for the particular EHR system function defined by the Elements of this Entry. The
sensitivity is specified in accordance with Section 6.1 of this part standard.">
                    text = <"maximum sensitivity">
                >
                ["at0027"] = <
                    description = <"The maximum sensitivity granted for access to EHR
data">
                    text = <"access">
                >
                ["at0028"] = <
                    description = <"The maximum sensitivity at which new Record Components
of this type may be committed to the EHR">
                    text = <"create">
                >
                ["at0029"] = <
                    description = <"The maximum sensitivity of Record Component that the
requestor may modify or logically delete">
                    text = <"revise">
                >
                ["at0030"] = <
                    description = <"The maximum sensitivity of Record Component that the
requestor may choose to share with other parties">
                    text = <"communicate">
                >
                ["at0031"] = <
                    description = <"The instruction within this policy about access to
former versions of EHR data">
                    text = <"version history">
                >
                ["at0032"] = <
                    description = <"A Boolean indicating if this class of requestor should
be granted access to former versions of a revised Record Component, if they do have access
to the revised instance">
                    text = <"all versions">
                >
                ["at0033"] = <
                    description = <"A set of additional rules, which might be specified
locally and/or required to comply with local or national policy or legislation">
                    text = <"other rules">
                >
                ["at0034"] = <
                    description = <"A specific (locally-defined) access rule">
                    text = <"access rule">
                >
        >
    >
>
```

:

6.4 UML representation of the archetype of the access policy COMPOSITION

The UML diagram in Figure 5 is a logically equivalent representation to the ADL Archetype specified in 6.3. It is included as an option for conformance in this part of ISO 13606 to support the communication of access policy information in accordance with ISO/TS 22600.

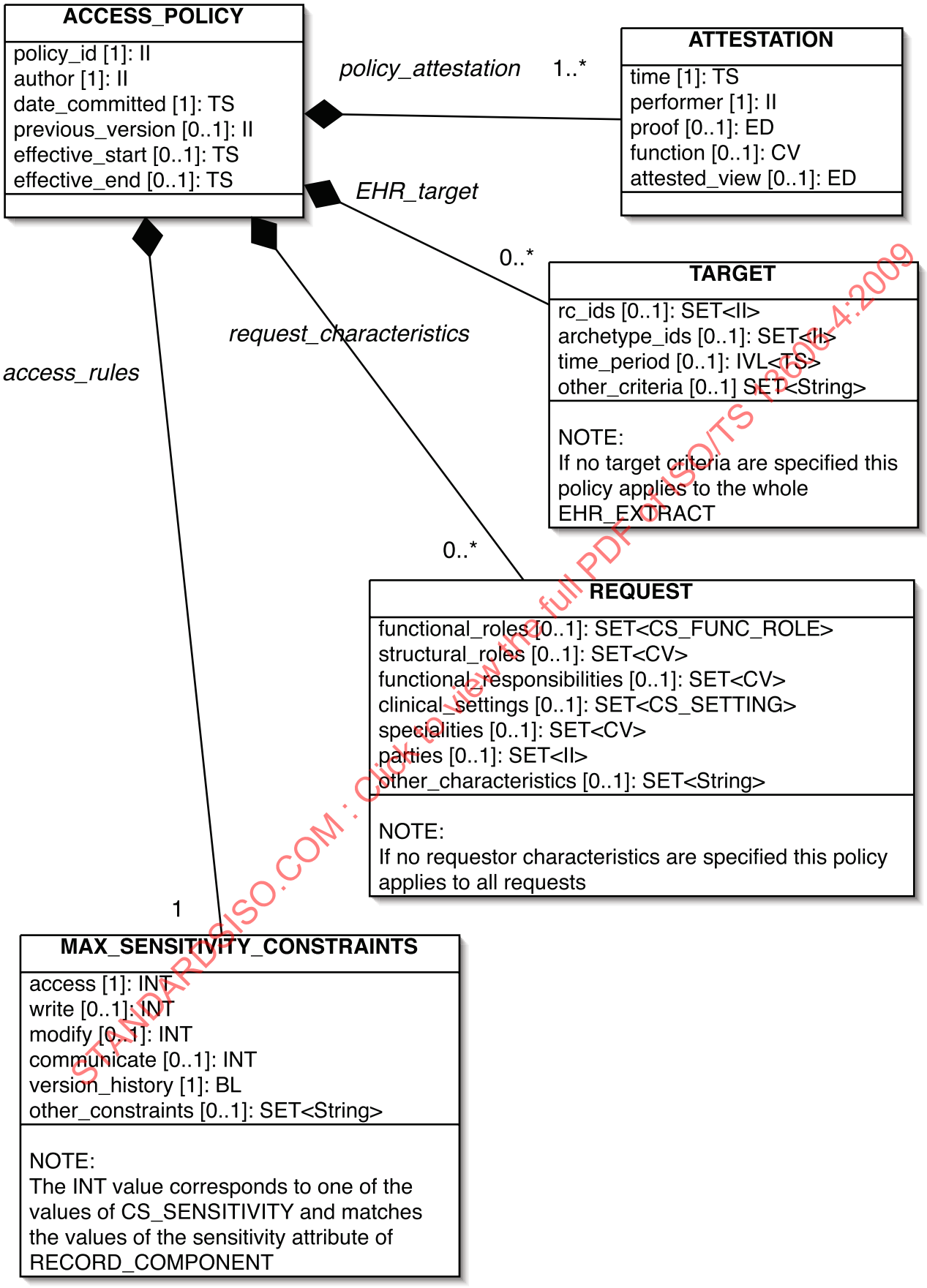


Figure 5 — UML representation of the access policy model

7 Representation of audit log information —EHR_AUDIT_LOG_EXTRACT model

Figure 6 shows the information model to be used to communicate an EHR access log, if it is a conformance requirement for this part of ISO 13606. An explanation of the classes and attributes is given below Figure 6.

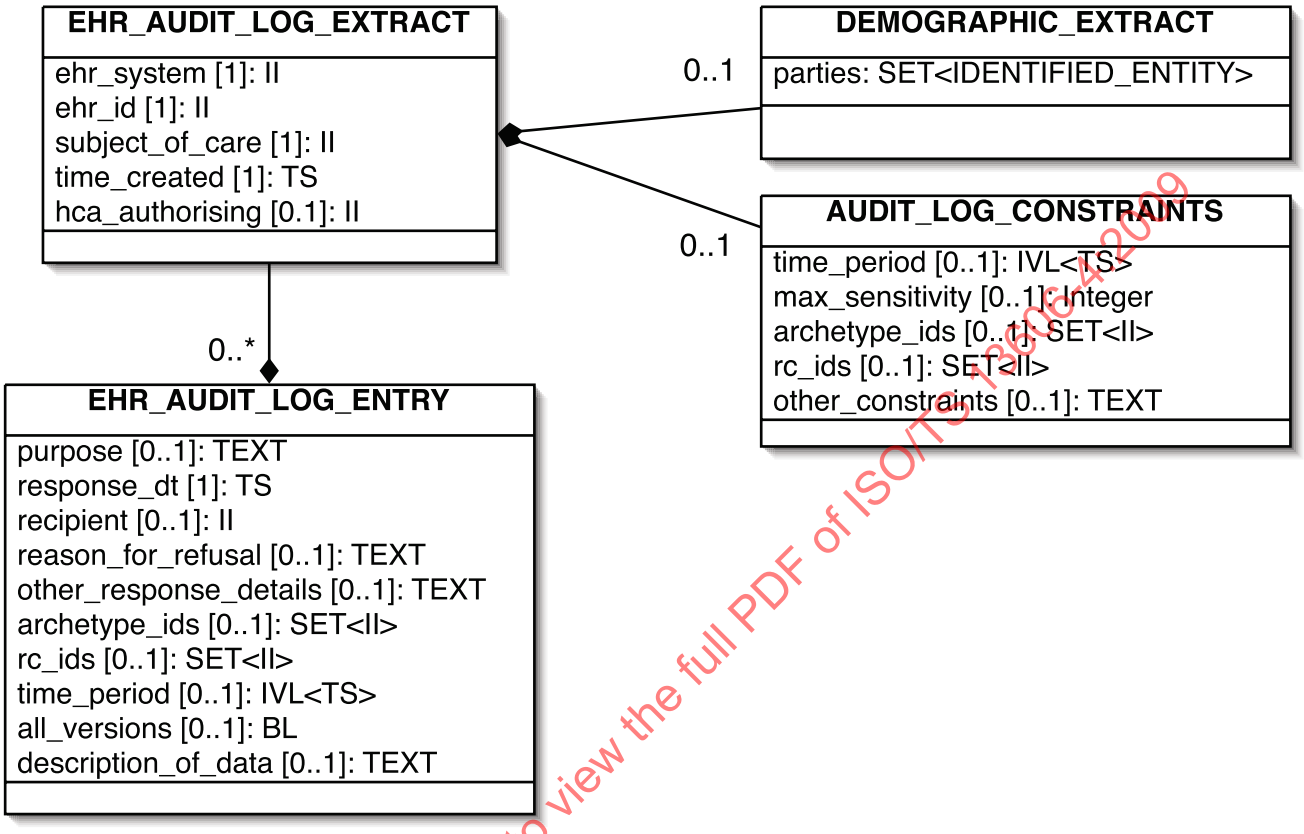


Figure 6 — UML model of the EHR audit log extract

EHR_AUDIT_LOG_EXTRACT
Root class containing the EHR audit log in a communicable form, as defined in this part of ISO 13606.

ehr_system [1]: II
Unique identifier of the EHR system from which the EHR has been accessed.

ehr_id [1]: II
Unique identifier of the electronic health record that has been accessed.

subject_of_care [1]: II
Unique identifier for the subject of care to whom the EHR relates.

time_created [1]: TS
Date and time that this audit log information was extracted from the audit log system.

hca_authorising [0.1]: II
Identifier of the party who has authorized the creation and communication of this audit log extract.

DEMOGRAPHIC_EXTRACT [0..1]

parties: SET<IDENTIFIED_ENTITY>
This class is identical to the class with a corresponding name in the EHR reference model defined in

ISO 13606-1. This same package is to be used to include the basic descriptive information of all parties identified in this audit log extract (the subject of care, healthcare agents, organizations, devices etc.).

AUDIT_LOG_CONSTRAINTS [0..1]
This class defines the filter that has been applied in generating this audit log extract, in response to a request for it.

time_period [0..1]: IVL<TS>
Time period which this audit log extract covers.

max_sensitivity [0..1]: Integer
Maximum sensitivity of RECORD_COMPONENT whose access is described in this audit log extract.

archetype_ids [0..1]: SET<II>
Set of archetypes to which this audit log extract is limited.

rc_ids [0..1]: SET<II>
Set of RECORD_COMPONENTS to which this audit log extract is limited.

other_constraints [0..1]: TEXT
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.

EHR_AUDIT_LOG_ENTRY [0..*]
EHR_AUDIT_LOG_EXTRACT contains a set of entries, each of which relates to one interaction with this EHR within this EHR system. An audit log entry contains information about the EHR data that was accessed, to whom, and when.

purpose [0..1]: TEXT
Description of the rationale for the EHR request.

response_dt [1]: TS
Date and time when the EHR system provided its response.

recipient [0..1]: II
Party to whom the EHR data was communicated. This might or might not be the person specified as recipient in the request.

reason_for_refusal [0..1]: TEXT
Description of the reason why the request was declined or only met in part. A text data type has deliberately been provided for this attribute, as a formal code set is not available.

other_response_details [0..1]: TEXT
Attribute may be used to represent any other details about the response, for example the description of any trigger events or other factors that gave rise to an EHR data “push” in the absence of any request.

archetype_ids [0..1]: SET<II>
Set of archetypes included in the EHR_EXTRACT.

rc_ids [0..1]: SET<II>
Set of RECORD_COMPONENTS included in the EHR_EXTRACT.

time_period [0..1]: IVL<TS>
Time period covered by the EHR_EXTRACT, if it was derived as a time period filter of the EHR.

all_versions [0..1]: BL
If all versions were included in the EHR_EXTRACT.

description_of_data [0..1]: TEXT
Any other details that describe the EHR_EXTRACT or constraints applied to its creation.

Annex A
(informative)

Illustrative access control example

The diagrams below provide an illustration of the way in which comparatively simple policies may 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,

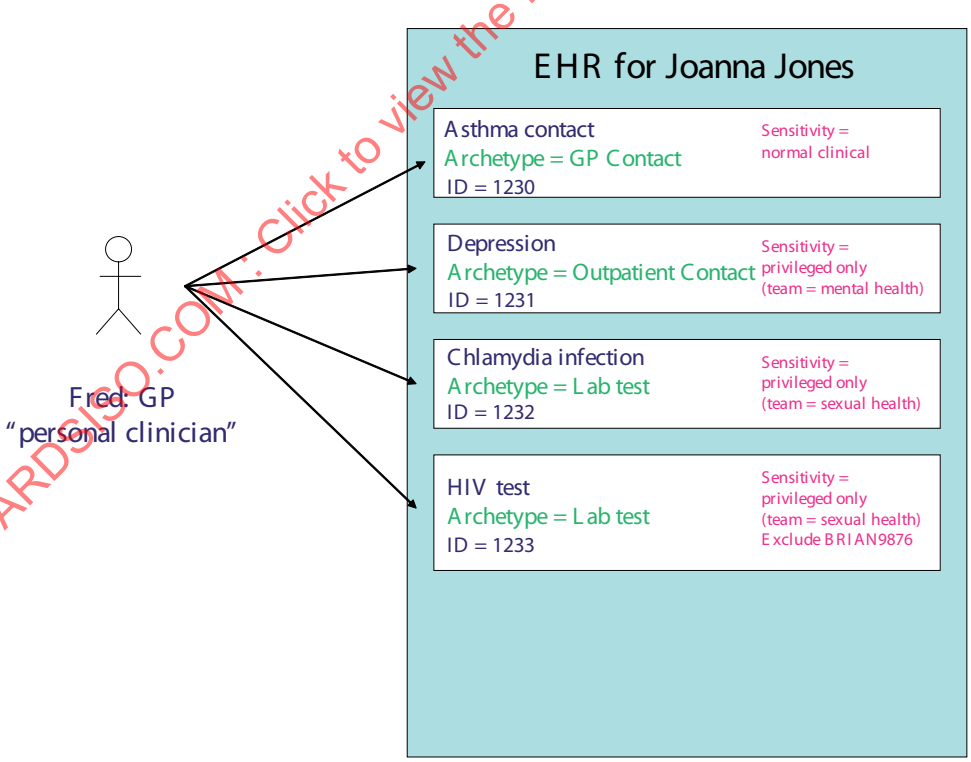
— an outpatient (ambulatory care) consultation for depression with a psychiatrist,

— a laboratory test performed in a sexual health clinic confirming the presence of a chlamydia infection and

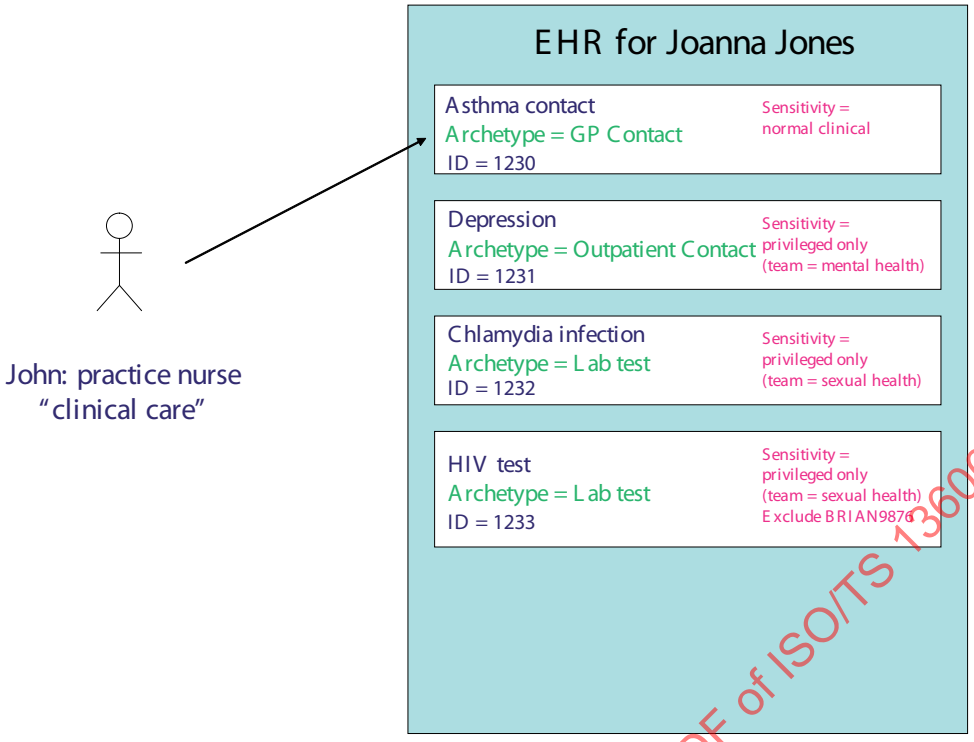
— an HIV test result.

Each of these has a defined sensitivity (in accordance with 5.1). The HIV test also references a policy by which a named party is denied access to this composition.

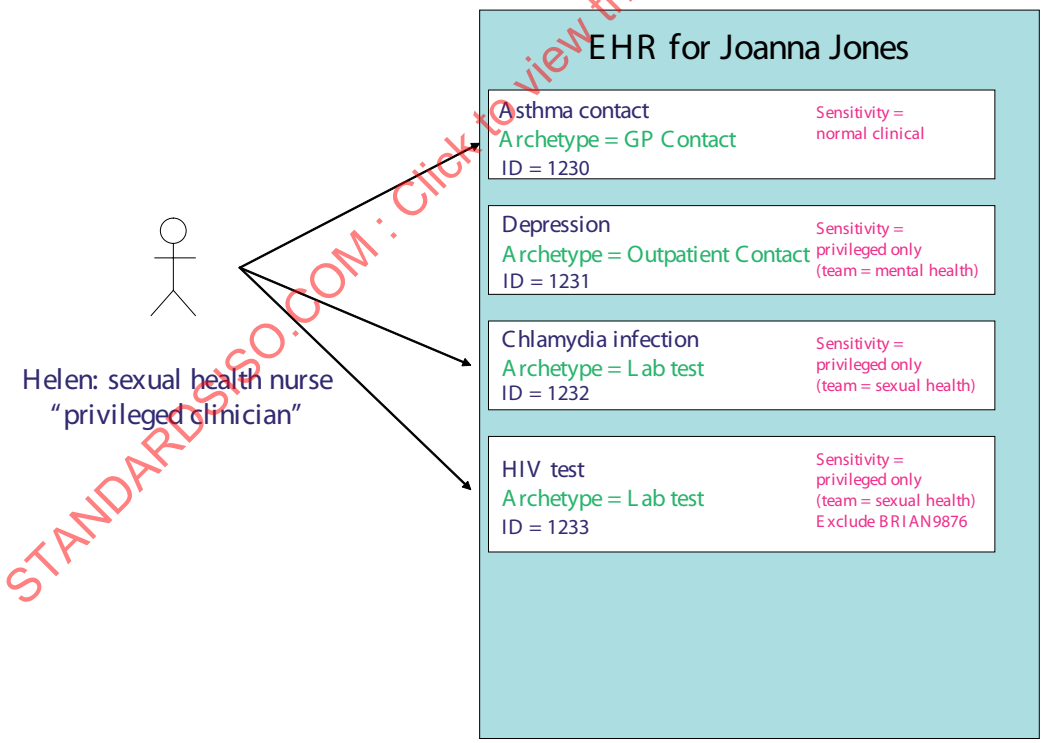
Fred is Joanna's general practitioner; he is able to access her EHR in the functional role of personal clinician. He is able to access all four of these compositions.



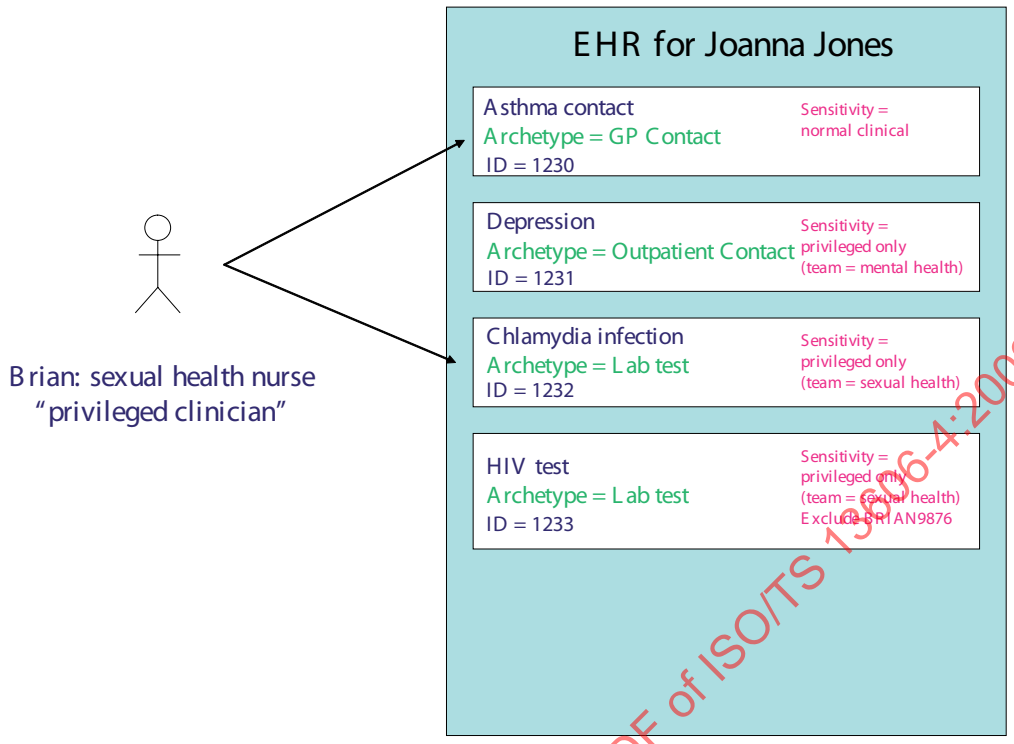
John is a practice nurse at the same general practice. His functional role is clinical care. This means that he is only able to access the asthma contact.



Helen works as a nurse in the sexual health clinic. She may have the functional role of privileged clinician, with her privilege defined as pertaining to the clinical setting of sexual health. She is therefore able to see the asthma contact and both sexual health clinic compositions (chlamydia test and HIV test results).



Brian works in the same setting as Helen, and would normally expect to access the same information as Helen. However, because he has been explicitly excluded from accessing the HIV test result he can only access two compositions in Joanna's EHR.



Joanna is only fifteen years old, and is concerned that her mother has legal (parental guardianship) rights to access her EHR. She does not wish her mother to know about her sexual activity, which would readily be inferred if her mother accessed the chlamydia or HIV test results, or even knew of their existence. Joanna has therefore authored a policy that applies to her EHR as a whole, and excludes her parents from access to any laboratory test results. This has the advantage that it will continue to apply to future test results, if for example a subsequent microbiology test is performed at the sexual health clinic or by her GP.

It is a complex ethical issue to determine if Joanna should be allowed to author such a policy, and under whose authority. National legislation may vary on this, but it might be permitted if she is judged to be of sufficient maturity and competence, or if attendance at a sexual health clinic confers such rights automatically. The purpose of this example is not to enter into such a debate, but to show how a general EHR policy can be defined for purposes such as this.