SLOVENSKI STANDARD

SIST EN 13606-4:2008

01-maj-2008

Nadomeġļa:

SIST ENV 13606-4:2003

Zdravstvena informatika - Komunikacija z elektronskimi zapisi na podroļju zdravstva - 4. del: Varnost

Health Informatics - Electronic health record communication - Part 4: Security

Medizinische Informatik - Kommunikation von Patientendaten in elektronischer Form - Teil 4: Sicherheit

Informatique de la santé - Communication des dossiers informatisés de santé - Partie 4 : Sécurité

Ta slovenski standard je istoveten z: **EN 13606-4:2007**

ICS:

35.240.80

SIST EN 13606-4:2008 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 13606-4

March 2007

ICS 35.240.80

Supersedes ENV 13606-4:2000

English Version

Health informatics - Electronic health record communication - Part 4: Security

Informatique de santé - Dossiers de santé informatisés communicants - Partie 4 : Exigences de sécurité et règles de distribution

Medizinische Informatik - Kommunikation von Patientendaten in elektronischer Form - Teil 4: Sicherheit

This European Standard was approved by CEN on 10 February 2007.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Ref. No. EN 13606-4:2007: E

Contents

Page

Foreword

This document (EN 13606-4:2007) has been prepared by Technical Committee CEN/TC 251 “Health informatics”, the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by September 2007, and conflicting national standards shall be withdrawn at the latest by September 2007.

This document supersedes ENV 13606-4:2000.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

Introduction

Challenge addressed by this Part Standard

The communication of electronic health records (EHRs) in whole or in part, within and across organisational boundaries, and sometimes across national borders, is challenging from a security perspective. Health records should be created, processed and managed in ways that 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. The EU Data Protection Directive [95/46/EC] and the Council of Europe Recommendation on the Protection of Medical Data R(97)5 provide an important legal basis for the requirements for security services as described in this standard. 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 wishes by which the data subject signifies his agreement to personal data relating to him being processed"). For international health record transfers EN 14484 (Health informatics - International transfer of personal health data covered by the EU data protection directive - High level security policy) and EN 14485 (Health informatics - Guidance for handling personal health data in international applications in the context of the EU data protection directive) provide policy guidance on how this may lawfully and safely be carried out.

Ideally, each fine grained entry in a patient's record should be capable of being associated with an access control list of persons who have rights to view that information, which has been generated or at least approved by the patient and that reflects 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 rights to access the data for reasons other than a duty of care (such as health service management, epidemiology and public health, consented research) but exclude any information that they do not need to see or which the patient feels is too personal for them to access. On the opposite side, the labelling by patients or their representatives of information as personal or private should ideally not hamper those who legitimately need to see the information in an emergency, nor accidentally result in genuine health care providers having such a filtered perspective that they are misled into managing the patient inappropriately. Patients' views on the inherent sensitivity 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 health care;
- numbers of health care 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 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;

- 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 health care 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 recognize that, for the foreseeable future, diversity will continue to exist across Europe on the specific approaches to securing EHR communications, including differing legislation, and that a highly prescriptive approach to standardization is not presently possible.

This European standard 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 Part 1 of this multipart standard, and defines specific information structures that are to be communicated as part of an EHR_EXTRACT defined in Part 1.

NOTE Some of the kinds of agreement necessary for the security of EHR communication are inevitably outside the scope of this standard. The complete protection of EHR communication requires attention to a large number of issues, many of which are not specific to health information. CEN/TC 251/WG III has been developing a series of standards related to health care security services and management, which should be applied when building EHR systems. Much of this work is now being done in co-operation between CEN and ISO/TC 215/WG 4 Health informatics/Security. There are a number of ongoing work items that have not been published at the time of writing this draft version of standard but which should become available before this standard is published, and will prove useful for the implementers of EHR systems. Some of these are:

- Joint CEN-ISO Work Item: ISO/TS 22600 Privilege Management and Access Control (PMAC),

- ISO Work Item: ISO/TS 21298 on Functional and Structural roles.

Communication scenarios

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

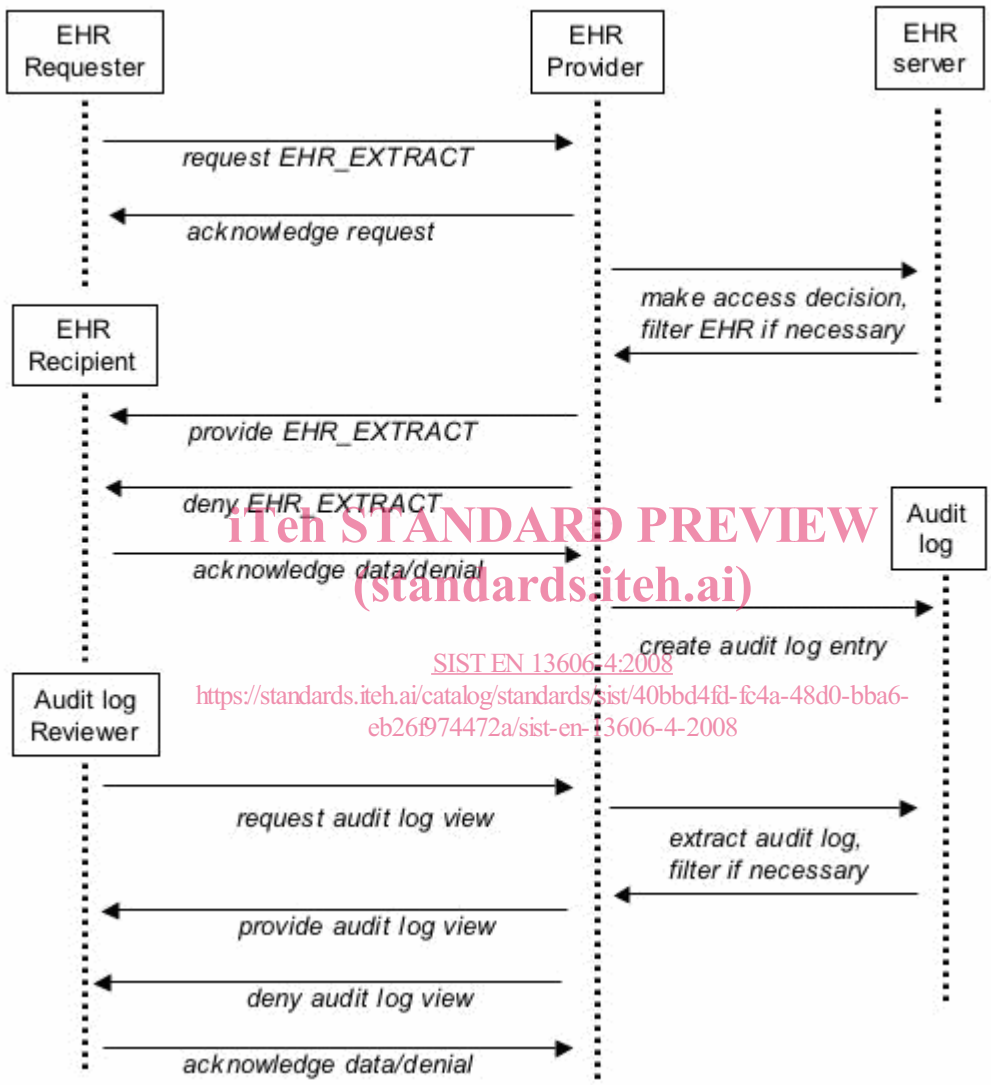

Figure 1 — Principal data flows and security-related business processes coved by this part-standard

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.

Request EHR data

This interaction is not always required (for example, EHR data might be pushed from Provider to Recipient as in the case of a discharge summary). The request interface needs to include a sufficient profile of the Requester to enable the EHR Provider to be in a position to make an access decision, to populate an audit log, and provide the appropriate data to the intended Recipient. In some cases the EHR Requester might not be the same party as the EHR Recipient – for example a software agent might trigger a notification containing

EHR data to be sent to a healthcare professional. In such cases it is the EHR Recipient's credentials that will principally determine the access decision to be made.

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

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

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

Acknowledge receipt of EHR_Request

No unique security considerations.

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 standard cannot dictate the overall set of policies that might influence the EHR Provider, potentially deriving from national, regional, organisation-specific, professional and other legislation.

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

This access decision is discussed in more detail in clause 6 of this part standard.

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 unique security considerations – the interface model will be defined in Part 5 of this standard.

Provide EHR_EXTRACT

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

The EHR_EXTRACT is required to conform to the Reference Model defined in Part 1 of this standard, and to the interface model defined in Part 5.

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

Acknowledge receipt of EHR_EXTRACT

No unique security considerations.

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 interfaces below.

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 standard, 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 6 of this part standard.

The interface model will be defined in Part 5 of this standard.

Provide EHR access log view

This is desirable practice, and requires an interoperable representation of such an entry (or set of entries). This interface is discussed in clause 6 of this part standard.

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 will be defined in Part 5 of this standard.

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 unique security considerations – the interface model will be defined in Part 5 of this standard.

Acknowledge receipt of EHR access log view

No unique security considerations.

Requirements and technical approach

The vision of research, industry and previous European 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 European R&D background work in these fields includes 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.

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 17799. This specifies the kinds of measures that should be taken to protect assets such as EHR data, and ways in which such data might safely be communicated as part of a distributed computing environment. A health specific guide to this general standard has been developed by ISO in co-operation with CEN (ISO/DIS 27799) Health informatics – Security management in health using ISO/IEC 17799. This will facilitate the formulation of common security polices across healthcare, and should help promote the adoption of interoperable security components and services.

For EHR communication across borders also to countries outside the European Union, guidance and security policy specifications are found in EN 14484 (Health informatics - International transfer of personal health data covered by the EU data protection directive - High level security policy) and EN 14485 (Health informatics - Guidance for handling personal health data in international applications in the context of the EU data protection directive). ISO 22857 provides similar information when an EU country is not involved.

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

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 must take place over protected networks, and an audit log must 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 health care, and this standard assumes that these services will be in place and used for every EHR communication.

The approach taken in drafting this part standard 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 standard therefore assumes that an overall security policy or set of policies conforming to ISO/IEC 17799 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 satisfying the provisions of EU Directive 94/95. Additional polices 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 standard.

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

The ISO Privilege Management and Access Control (PMAC) standard, ISO/TS 22600, being developed in WG 4 of ISO TC/215, 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. The standard 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 PMAC.

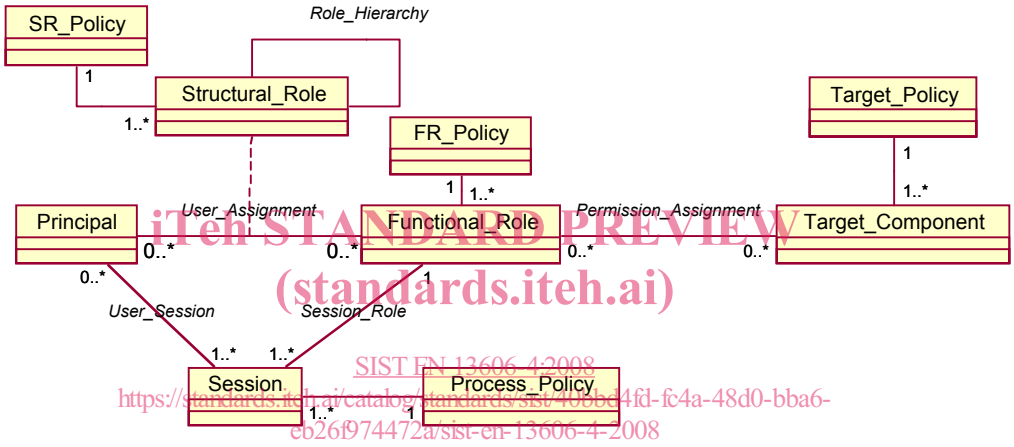

Figure 2 — Main concepts and policy types defined in Role Based Access Control

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 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 standard, 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, the PMAC standard 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-standard assumes that the PMAC 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 PMAC logical approach is technically implemented in any organization or region.

The PMAC standard is expected to define a generic (interoperable) policy model for Target Policies, but that part of the standard is not expected to be published until 2006 to 2007. This part standard for EHR Communications security therefore includes an informative model that may be used until that part of the PMAC standard is published and widely adopted.

As a complement to that emerging standard, a new Work Item within ISO proposes to define 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 standard recognizes that these and other standardized vocabularies will increasingly support rich interoperability of access policies, but cannot at this stage mandate the use of any particular controlled vocabulary since none exists in a standardized form.

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 Part 1 of this standard). The following table lists those requirements that apply most specifically to this part standard.

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 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	The 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

Generic EHR Access Policy model

In addressing these requirements within this standard, it is recognized 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 may 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 PMAC architecture. Some example factors that might be specified within such policies, and taken into account when making an EHR access decision, are listed below.

National, Professional, Organizational policies might be based upon, for example:

a) 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

b) Access characteristics:
   - date and time
   - location
   - physical device
   - network or other communications mechanism
   - mechanisms and extent of encryption in place
   - method of authentication used

c) 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 must be provided)

The whole spectrum of access policies in place at an organization is beyond the scope of this standard, but this part standard 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.