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

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

Käesolev Eesti standard EVS-EN 13606-4:2007 sisaldab Euroopa standardi EN 13606-4:2007 ingliskeelset teksti.	This Estonian standard EVS-EN 13606-4:2007 consists of the English text of the European standard EN 13606-4:2007.
Standard on kinnitatud Eesti Standardikeskuse 21.06.2007 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.	This standard is ratified with the order of Estonian Centre for Standardisation dated 21.06.2007 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.
Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuupäev on 28.03.2007.	Date of Availability of the European standard text 28.03.2007.
Standard on kättesaadav Eesti standardiorganisatsioonist.	The standard is available from Estonian standardisation organisation.

ICS 35.240.80

Võtmesõnad:

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.

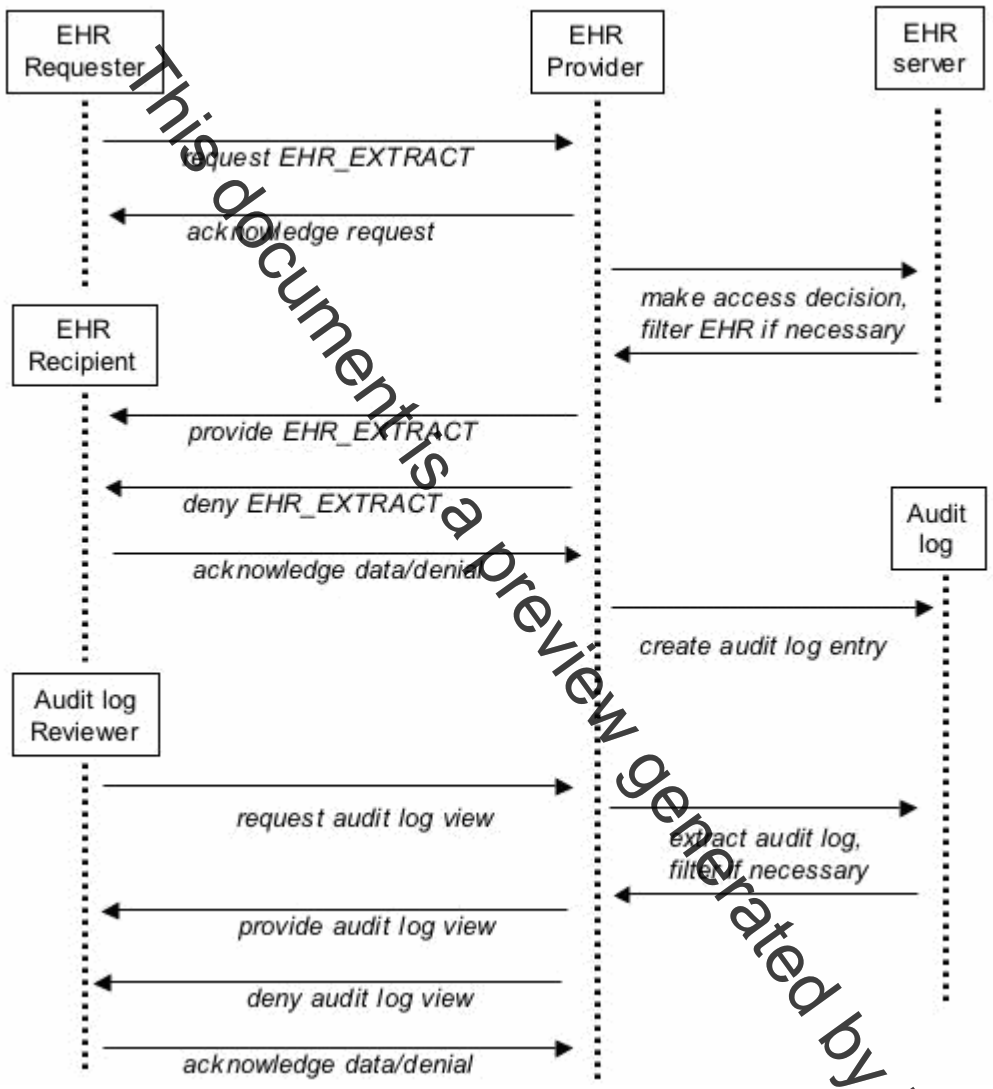

Figure 1 — Principal data flows and security-related business processes coved by this part-standard

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.