INTERNATIONAL STANDARD

ISO 13606-4

First edition
2019-06

Health informatics — Electronic health record communication —

Part 4: Security

Informatique de santé — Communication du dossier de santé informatisé —
Partie 4: Sécurité

Reference number
ISO 13606-4:2019(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

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

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

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

— Functional Roles

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

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

— Access policy model

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

— Audit log model

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

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

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

Introduction

0.1 General

This document, is part of a five-part standard series, published jointly by CEN and ISO through the Vienna Agreement. In this document, dependency upon any of the other parts of this series is explicitly stated where it applies.

0.2 Challenge addressed by this document

The communication of electronic health records (EHRs) in whole or in part, within and across organisational boundaries, and sometimes across national borders, is challenging from a security perspective. Health records should be created, processed and managed in ways that assure the confidentiality of their contents and legitimate control by patients in how they are used. Around the globe, these principles are progressively becoming enshrined in national data protection legislation. These instruments declare that the subject of care has the right to play a pivotal role in decisions on the content and distribution of his or her electronic health record, as well as rights to be informed of its contents. The communication of health record information to third parties should take place only with patient consent (which can be any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed). More details can be found in ISO 22600-3. For EHR communication across national borders, ISO 22857 provides guidance that can be used to define appropriate security policy specifications.

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

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

— the large number of health record entries made on a patient during the course of modern health care;

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

— the large number of organisations with which a patient might come into contact during his or her lifetime;

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

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

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

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

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

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

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

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

The main principles of the approach to standards development in the area of EHR communications access control are to match the characteristics and parameters of a request to the EHR provider's policies, and to any access control or consent declarations within the specified EHR, to maintain appropriate evidence of the disclosure, and to make this capable of automated processing. In practice, efforts are in progress to develop international standards for defining access control and privilege management systems that would be capable of computer-to-computer negotiation. However, this kind of work is predicated upon health services agreeing a mutually consistent framework for defining the privileges they wish to assign to staff, and the spectrum of sensitivity they offer for patients to define within their EHRs. This requires consistency in the way the relevant information is expressed, to make this sensibly scalable at definition-time (when new EHR entries are being added), at run-time (when a whole EHR is being retrieved or queried), and durable over a patient's lifetime. It is also important to recognize that, for the foreseeable future, diversity will continue to exist between countries on the specific approaches to securing EHR communications, including differing legislation, and that a highly prescriptive approach to standardization is not presently possible.

This document therefore does not prescribe the access rules themselves. It does not specify who should have access to what and by means of which security mechanisms; these need to be determined by user communities, national guidelines and legislation. However, it does define a basic framework that can be used as a minimum specification of EHR access policy, and a richer generic representation for the communication of more fine-grained detailed policy information. This framework complements the overall architecture defined in ISO 13606-1, and defines specific information structures that are to be communicated as part of an EHR_EXTRACT defined in ISO 13606-1. Some of the kinds of agreement necessary for the security of EHR communication are inevitably outside the scope of this document, and are covered more extensively in ISO 22600 (Privilege Management and Access Control).

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

0.3 Communication scenarios

0.3.1 Data flows

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

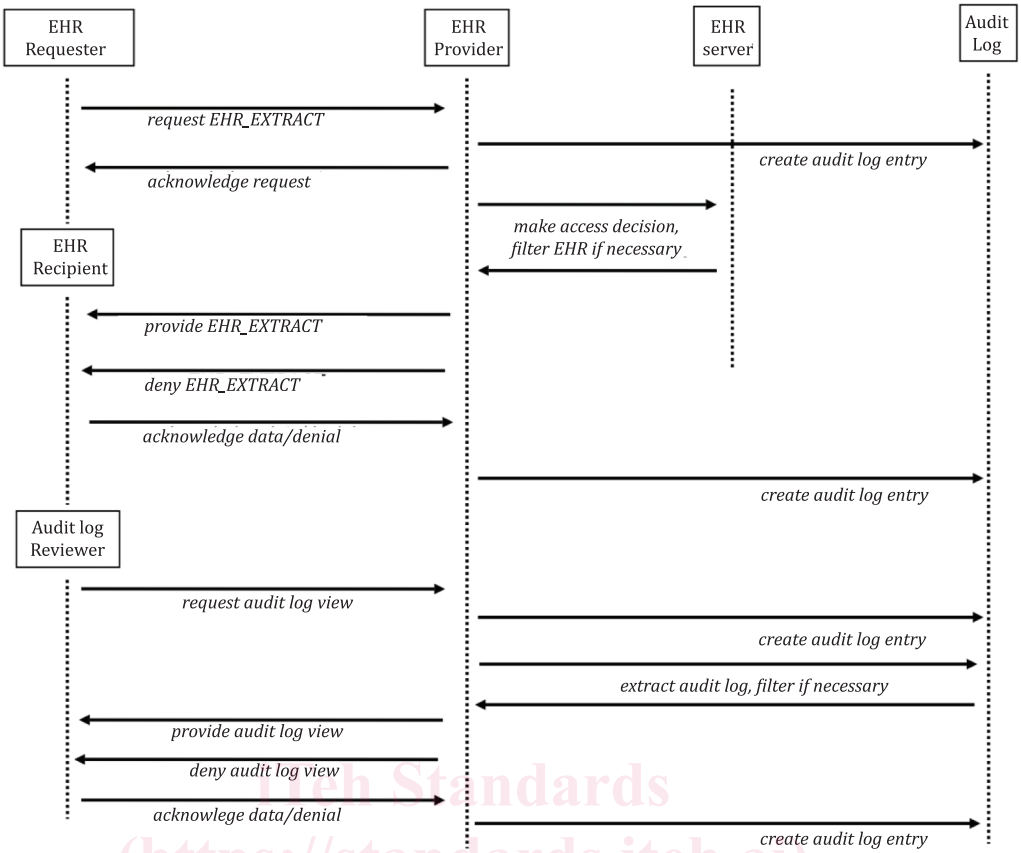

Figure 1 — Principal data flows and security-related business processes covered by this document

The EHR Requester, EHR Recipient and Audit Log Reviewer might be healthcare professionals, the patient, a legal representative or another party with sufficient authorization to access healthcare information. Both the EHR_EXTRACT and the audit log, if provided, might need to be filtered to limit the disclosure to match the privileges of the recipient. This aspect of access control is discussed later in this introduction (all parties shown here will need to maintain an audit log, not just the EHR Provider. However, for readability the other audit log processes are not shown or described here).

The following subclauses describe each data flow in Figure 1.

0.3.2 Request EHR data

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

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

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

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

0.3.3 Generate EHR access log entry

This is assumed practice in any EHR system, but it is not specified as a normative interface because of the diverse approaches and capabilities in present-day systems. The internal audit systems within any EHR system are not required to be interoperable except in support of the model defined in Clause 8 of this document and the corresponding interface defined in ISO 13606-5.

0.3.4 Acknowledge receipt of the EHR request

No healthcare-specific security considerations.

0.3.5 Make access decision, filter EHR data

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

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

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

This access decision is discussed in more detail in Clause 7.

0.3.6 Deny provision of the EHR_EXTRACT

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

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

0.3.7 Provide the EHR_EXTRACT

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

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

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

0.3.8 Acknowledge receipt of EHR_EXTRACT

No healthcare-specific security considerations.

0.3.9 Generate EHR access log entry

As described in 0.3.3.

0.3.10 Request EHR access log view

This is now considered to be desirable practice, to enable a patient to discover who has accessed part or all of his/her EHR in an information-sharing environment. The scope of this interface, as defined in this document, is to request a view of the audit log that informs the recipient about who has accessed what parts of his or her EHR within a given EHR system, and when. This interface is not intended to support situations where a full inspection of an audit log is required for legal purposes or for other investigations. This interface is discussed in Clause 6.

The interface model is defined in ISO 13606-5.

0.3.11 Generate EHR access log entry

As described in 0.3.3.

0.3.12 Provide EHR access log view

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

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

The interface model is defined in ISO 13606-5.

0.3.13 Deny EHR access log view

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

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

0.3.14 Acknowledge receipt of EHR access log view

No healthcare-specific security considerations.

0.3.15 Generate EHR access log entry

As described in 0.3.3.

0.4 Requirements and technical approach

0.4.1 Generic healthcare security requirements

The most widely accepted requirements for an overall security approach in domains handling sensitive and personal data are published in ISO/IEC 27002. This specifies the kinds of measures that should be taken to protect assets such as EHR data, and ways in which such data might safely be communicated as part of a distributed computing environment. A health specific guide to this general standard has been published in ISO 27799 (Health informatics – Security management in health using ISO/IEC 27002). This will facilitate the formulation of common security polices across healthcare, and should help promote the adoption of interoperable security components and services. ISO 22600 (Health informatics — Privilege management and access control) defines a comprehensive architectural approach to formally and consistently defining and managing such policies. For EHR communication across national borders ISO 22857 provides guidance that can be used to define appropriate security policy specifications.

The exact security requirements that need to be met to permit any particular EHR communication instance will be governed by a number of national and local policies at both the sending and receiving sites, and at any intermediate links in the communications chain. Many of these policies will apply to healthcare communications in general, and will vary between countries and clinical settings in ways that cannot and should not be directed by this document. The approach taken in drafting this document has therefore been to assume that generic security policies, components and services will contribute to

a negotiation phase (the *access decision*) prior to sanctioning the communication of an EHR Extract, and will protect the actual EHR data flows.

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

0.4.2 Relationship to other related security standards

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

ISO 22600 (all parts) defines a generic logical model for the representation of the privileges of principals (entities), of access control policies that pertain to potential target objects, and of the negotiation process that is required to arrive at an access decision. Figure 2 depicts the concepts of Role Based Access Control defined in ISO 22600 (all parts).

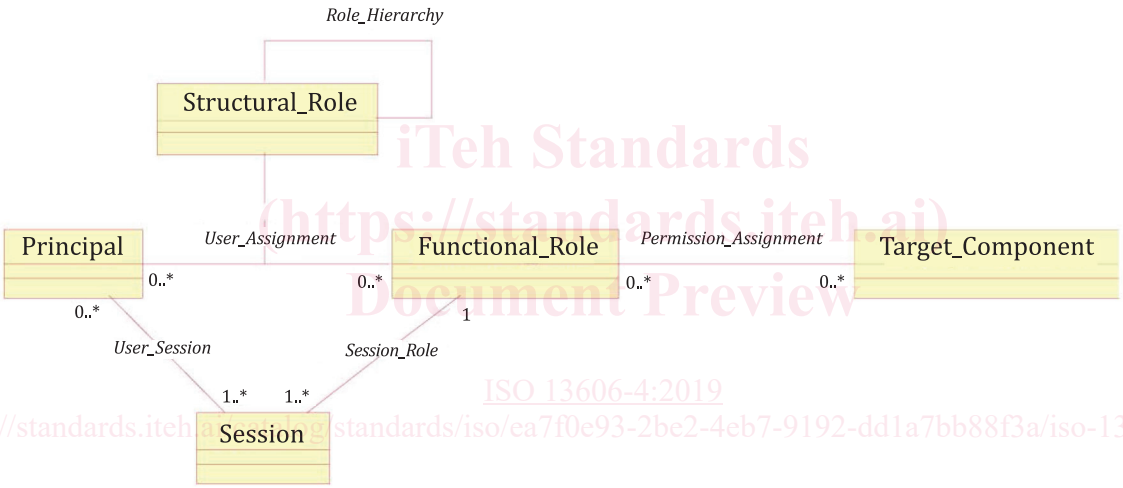

Figure 2 — Main concepts and policy types defined in Role Based Access Control [ISO 22600 (all parts)]

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

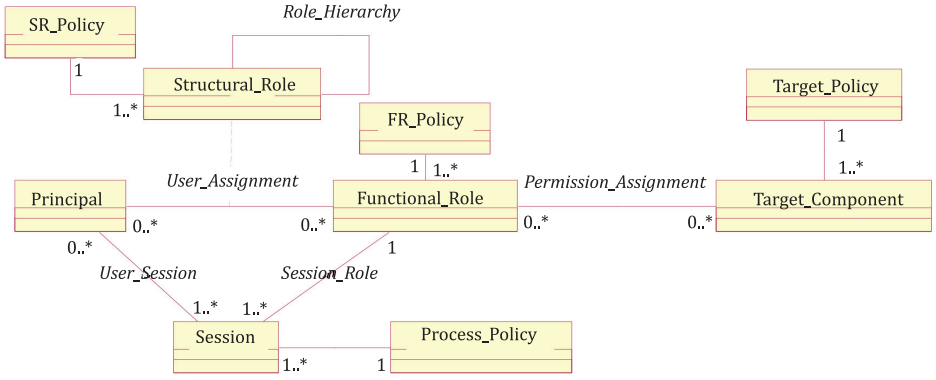

Figure 3 — Policy-driven RBAC Schema

As illustrated in Figure 3, principals (persons, agents etc.) are mapped to one or more Functional Roles, which will be influenced by the Structural Roles that they are permitted to hold. For example, a person who is medically qualified and a specialist in child health might hold one or more Structural Roles (such as Consultant Paediatrician at a hospital, Head of Child Screening for the region). Those Structural Roles might permit him or her at times to act with the Functional Role of Personal Clinician to a patient. The Functional Role might be persistent, or limited to a single user session. Functional Roles are mapped to permissions to perform particular operations (such as writing new entries in an EHR) and to particular objects (such as the EHR data which that role-holder is permitted to view).

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

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

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

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

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

05 EHR access policy model

0.5.1 Overall approach

In the ISO 13606-1 Reference Model every COMPOSITION within the EHR_EXTRACT includes an optional access_policy_ids attribute to permit references to such policies to be made at any level of granularity within the EHR containment hierarchy. Every COMPOSITION may therefore reference any number of access policies or consent declarations that define the intended necessary privileges and profiles of principals (users, agents, software, devices, delegated actors etc.) for future access to it. The information model in Clause 7 for representing and communicating access policy information has been deliberately kept very generic, to allow for the diversity of policy criteria that will be stipulated in different countries and regional healthcare networks. Standardized vocabularies for some of the main properties of the model are defined as default term lists. Although it is recommended that these be adopted whenever they are suitable, it is recognised that jurisdictions might have requirements or legislation or existing investments that mean that they cannot adopt these internationally-standardised term lists. This document therefore permits jurisdictions to declare conformance using alternative term lists.

Health and care environments increasingly comprise complex networks of agencies and actors from traditional healthcare settings, social care, informal carers and voluntary agencies (such as welfare charities) patients themselves, families and sometimes their social networks. All of these might at

times establish agreements to permit data sharing of personal health data. Given the dynamic nature of this "virtual care team" it might not be practical for these data sharing agreements to be negotiated in traditional human to human document based ways. It is therefore likely that such agencies will establish framework agreements that specify in advance the standards they each comply with, any mappings between their respective domains of privilege and how data are to be handled within each such privilege domain. As stated above, this policy model permits jurisdictions to instead declare alternative term lists that they will use. This allows for some flexibility in adoption of this document, recognising that complex data sharing environments might need to establish new, potentially richer, vocabularies to describe the wider range of actors and roles in that environment.

A number of existing and legacy systems might not be able to incorporate richly-defined policy specifications, and many healthcare regions might not be in a position to define such policies for some years. Therefore, as a complement to the overall policy model in Clause 7, this document defines two vocabularies that can provide a minimum basis for making an access policy decision, and ensure a basic level access policy interoperability, albeit at a coarse-grained level.

These two vocabularies are:

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

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

0.5.2 Defining 'Need to Know' when handling EHR data

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

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

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

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

