
**Health informatics — Electronic
health record communication —**

**Part 4:
Security**

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

iteh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 13606-4:2019

<https://standards.iteh.ai/catalog/standards/iso/ea7f0e93-2be2-4eb7-9192-dd1a7bb88f3a/iso-13606-4-2019>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 13606-4:2019

<https://standards.iteh.ai/catalog/standards/iso/ea7f0e93-2be2-4eb7-9192-dd1a7bb88f3a/iso-13606-4-2019>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviations	2
5 Conformance	2
6 Record Component Sensitivity and Functional Roles	3
6.1 RECORD_COMPONENT sensitivity	3
6.2 Functional roles	3
6.3 Mapping of Functional Role to COMPOSITION sensitivity	4
7 Representing access policy information within an EHR_EXTRACT	4
7.1 Overview	4
7.2 UML representation of the archetype of the access policy COMPOSITION	6
7.2.1 Access policy	7
7.2.2 Target	7
7.2.3 Request criterion	8
7.2.4 Sensitivity constraint	9
7.2.5 Attestation information	10
7.3 Archetype of the access policy COMPOSITION	11
8 Representing audit log information	11
8.1 General	11
8.1.1 EHR audit log extract	11
8.1.2 Audit log constraint	12
8.1.3 EHR audit log entry	13
8.1.4 EHR extract description	14
8.1.5 Demographic extract	15
Annex A (informative) Illustrative access control example	16
Annex B (informative) Relations of ISO 13606-4 to alternative approaches	20
Bibliography	22

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

ISO 13606-4:2019

<https://standards.iteh.ai/catalog/standards/iso/ea7f0e93-2be2-4eb7-9192-dd1a7bb88f3a/iso-13606-4-2019>

- 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 sensitivity¹⁾ 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.