International

ISO 13606-4

Health informatics — Electronic health record communication —

Part 4: Security

Informatique de santé — Communication du dossier de santé informatisé —

Partie 4: Sécurité

Second edition
2026-08

Reference number
ISO 13606-4:2026(en)

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

Published in Switzerland

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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of 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 www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 251, *Health informatics*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO 13606-4:2019 [1]), of which it constitutes a minor revision. The changes are as follows:

— the tables in Clause 7 and Clause 8 have been numbered;

— the examples in Annex B have been anonymized;

— corrections were made to Clause 2 and Clause 3 to reflect the technical content of the document.

A list of all parts in the ISO 13606 [2] 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.

0.1 General

This document is part of a series including five parts. 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 subjects of care 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 their EHR, as well as the right to be informed of its contents. The communication of health record information to third parties should normally take place only with consent from the subject of care (which can be any freely-given specific and informed indication of their wishes, by which the data subject signifies their agreement to personal data relating to them being processed in an ethically-acceptable way) . More details can be found in ISO 22600-3 [3]. For EHR communication across national borders, ISO 22857 [4] provides guidance that can be used to define appropriate security policy specifications.

Ideally, each fine-grained entry in a subject of care's record should only be accessed by those persons who have permissions to view that information, specified by or approved by the subject of care and reflecting the dynamic nature of the set of persons with legitimate duty of care towards the subject of care through their 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 subject of care feels is too personal for them to access. On the opposite side, the labelling by subjects of care or their representatives of information as personal or private should ideally not hamper those who legitimately need to see the information in an emergency, nor accidentally result in genuine healthcare providers having such a filtered perspective that they are misled into managing the subject of care inappropriately. Subject of care's views on the inherent sensitivity[1)] of entries in their health records can evolve over time, as their personal health anxieties alter or as societal attitudes to health problems change. Subjects of care 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 subject of care during the course of modern healthcare;

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

— the large number of healthcare organisations with which a subject of care can come into contact during their lifetime;

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

— the difficulty of determining how important a single health record entry can be to the future care of a subject of care, 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 the characteristic of a resource (EHR data) that implies its value or importance (and by implication the extent of confidentiality and therefore to the functional roles that should have access to it).

— 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 subjects of care to have their consent for disclosure recorded and respected;

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

To support interoperable EHRs, and seamless communication of EHR data between healthcare providers, the negotiation required to determine if a given Requester for EHR data should be permitted to receive the data should be capable of automation. If automated negotiation 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 the overall access decision process 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 subjects of care 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 subject of care'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 [5], and defines specific information structures that are to be communicated as part of an EHR_EXTRACT defined in ISO 13606-1 [5]. 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 the ISO 22600 [6] series.

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 [7] . 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 are 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.

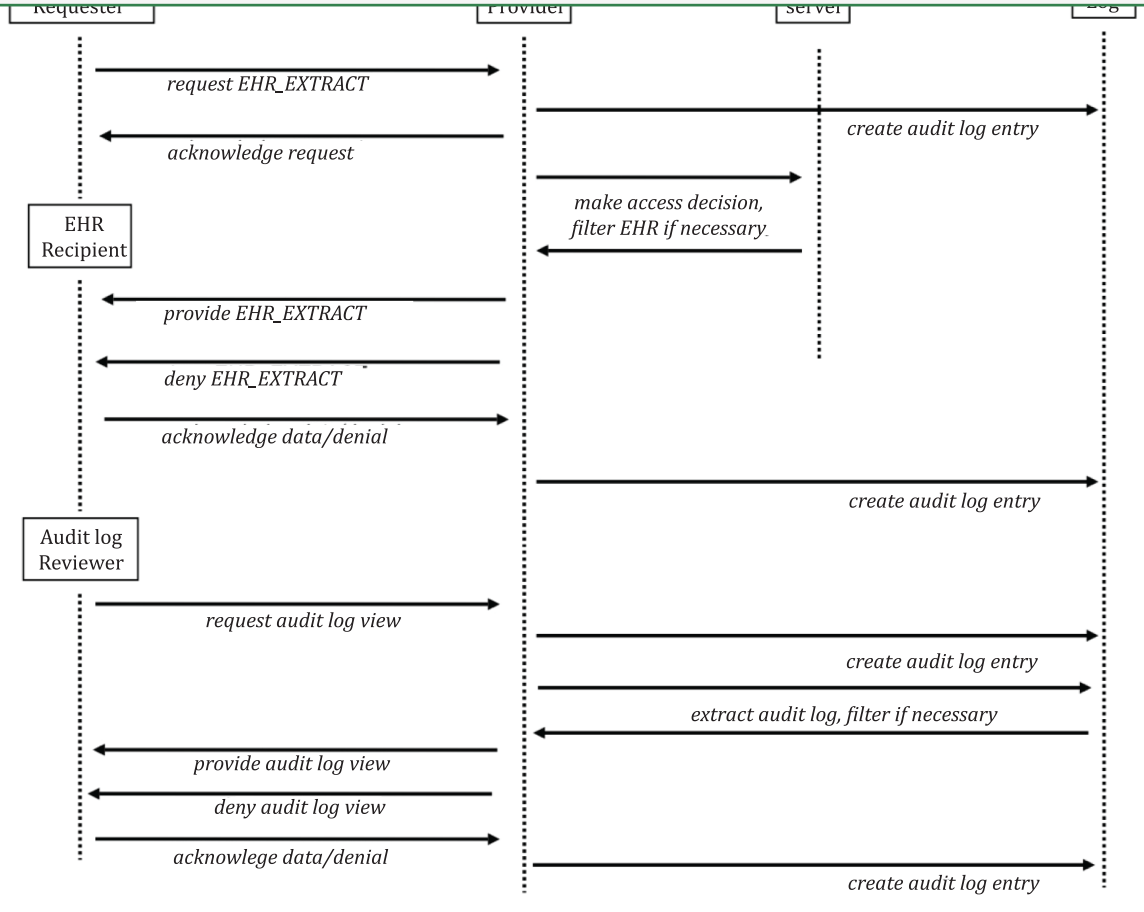

Figure 1 — Principal data flows and security-related business processes covered by this document

The EHR Requester, EHR Recipient and Audit Log Reviewer can be healthcare professionals, the subject of care, 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 subject of care, 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.