First edition
2017-02

Corrected version
2017-04

Health informatics — Functional and structural roles

Informatique de santé — Rôles fonctionnels et structurels

Reference number
ISO 21298:2017(E)

COPYRIGHT PROTECTED DOCUMENT

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

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 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 first edition of ISO 21298 cancels and replaces ISO/TS 21298:2008, which has been technically revised.

The committee responsible for this document is ISO/TC 215, *Health informatics*.

This corrected version incorporates the following correction:

— replacement of Figure 2.

Introduction

This document contains a specification for encoding information related to roles for health professionals and consumers. At least five areas have been identified where a model for encoding role information is needed.

a) **Privilege management and access control**: role-based access control is not possible without an effective means of recording role information for healthcare actors.

b) **Directory services**: structural roles are usefully recorded within directories of healthcare providers (see for example, ISO 21091).

c) **Audit trails**: functional roles are usefully recorded within audit trails for health information applications.

d) **Public key infrastructure (PKI)**: The ISO 17090 series allows for the encoding of healthcare roles in certificate extensions, but no structured vocabulary for such roles is specified. This document identifies such a coded vocabulary.

e) **Purpose of use**: A role specification determines for what purposes healthcare information can be used. Purposes of use are tied to specific roles in many cases (see for example, ISO 21091).

In addition to these security-related applications, there are several other possible applications of this standard, such as follows.

— **Clinical care provision**: finding and identifying the right professional for a health service.

— **Support of care**: billing of healthcare services.

— **Communication management**: directing healthcare-related messages by means of a specific role.

— **Health service management and quality assurance**: defining the purpose of use for specific data.

This document is complementary to other relevant standards that also describe and define roles for the purpose of access control. It extends the model through the separation of role and policy. This separation allows for a richer and more flexible capability to instantiate business rules across multiple domains and jurisdictions. Backward compatibility with ANSI International Committee for Information Technology Standards (INCITS) and HL7 RBAC (Role-Based Access Control) is provided through simplification by combining policy and role into a single construct.

The role concepts defined in this document are referenced and reused in many international standards created, for example, by ISO, CEN, HL7 International. Examples are ISO 22600, Reference [9], Reference [10] and Reference [11].

The European Commission and the EU Parliament have established a Professional Qualifications Directive (2005/36/EC) defining medical specialties (see http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02005L0036-20140117&from=EN).

Annex A provides ISOCO-08 sample mapping while Annex B provides sample certificate profile for regulated healthcare professionals.