

SLOVENSKI STANDARD oSIST prEN ISO 27789:2020

01-junij-2020

Zdravstvena informatika - Revizijske sledi za elektronske zdravstvene zapise (ISO/DIS 27789:2020)

Health informatics -- Audit trails for electronic health records (ISO/DIS 27789:2020)

Medizinische Informatik - Audit-Trails für elektronische Gesundheitsakten (ISO/DIS 27789:2020)

iTeh STANDARD PREVIEW

Informatique de santé -- Historique d'expertise des dossiers de santé informatisés (ISO/DIS 27789:2020)

oSIST prEN ISO 27789:2020

Ta slovenski standard je istovete n z log/standr EN ISO 427789^{2-4236-8c90-86cb761b507}/osist-pren-iso-27789-2020

ICS:

35.240.80 Uporabniške rešitve IT v IT applications in health care

zdravstveni tehniki technology

oSIST prEN ISO 27789:2020 en,fr,de

oSIST prEN ISO 27789:2020

iTeh STANDARD PREVIEW (standards.iteh.ai)

DRAFT INTERNATIONAL STANDARD ISO/DIS 27789

ISO/TC **215** Secretariat: **ANSI**

Voting begins on: Voting terminates on:

2020-04-17 2020-07-10

Health informatics — **Audit trails for electronic health records**

Informatique de santé — Historique d'expertise des dossiers de santé informatisés

ICS: 35.240.80

iTeh STANDARD PREVIEW (standards.iteh.ai)

oSIST prEN ISO 27789:2020 https://standards.iteh.ai/catalog/standards/sist/ab3842db-a6a2-4236-8c90-8f6cb761b507/osist-pren-iso-27789-2020

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING



Reference number ISO/DIS 27789:2020(E)

iTeh STANDARD PREVIEW (standards.iteh.ai)

oSIST prEN ISO 27789:2020 https://standards.iteh.ai/catalog/standards/sist/ab3842db-a6a2-4236-8c90-8f6cb761b507/osist-pren-iso-27789-2020



COPYRIGHT PROTECTED DOCUMENT

© ISO 2020

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

iii

Introduction	Contents				
1 Scope 1 2 Normative references 1 3 Terms and definitions 1 4 Symbols and abbreviated terms 5 5 Requirements and uses of audit data 5 5.1 Ethical and formal requirements 5 5.1.1 General 5 5.1.2 Access policy 5 5.1.3 Unambiguous identification of information system users 5 5.1.4 User roles 5 5.1.5 Secure audit records 6 5.2 Uses of autit data 6 5.2.1 Governance and supervision 6 5.2.2 Subjects of care exercising their rights 6 5.2.3 Healthcare provider's ethical or legal proof of action 6 6 Trigger events 7 6.1 General Tell STANDARD PREVIEW 7 6.2 Details of the event types and their contents 7 6.2.1 Access events to title personal health information 7 6.2.2 Query events to the personal health information 7 7.2 Trigger events dentification of the personal health information 8 7.2 Trigger event identification of the personal health information 9 7	Fore	eword		v	
1 Scope 1 2 Normative references 1 3 Terms and definitions 1 4 Symbols and abbreviated terms 5 5 Requirements and uses of audit data 5 5.1 Ethical and formal requirements 5 5.1.1 General 5 5.1.2 Access policy 5 5.1.3 Unambiguous identification of information system users 5 5.1.4 User roles 5 5.1.5 Secure audit records 6 5.2 Uses of autit data 6 5.2.1 Governance and supervision 6 5.2.2 Subjects of care exercising their rights 6 5.2.3 Healthcare provider's ethical or legal proof of action 6 6 Trigger events 7 6.1 General Tell STANDARD PREVIEW 7 6.2 Details of the event types and their contents 7 6.2.1 Access events to title personal health information 7 6.2.2 Query events to the personal health information 7 7.2 Trigger events dentification of the personal health information 8 7.2 Trigger event identification of the personal health information 9 7	Intr	oductio	on .	vi	
2 Normative references					
3 Terms and definitions		-			
4 Symbols and abbreviated terms 5 5 Requirements and uses of audit data 5 5.1 Ethical and formal requirements 5 5.1.1 General 5 5.1.2 Access policy 5 5.1.3 Unambiguous identification of information system users 5 5.1.4 User roles 5 5.1.5 Secure audit records 6 5.2 Uses of audit data 6 5.2.1 Governance and supervision 6 5.2.2 Subjects of care exercising their rights 6 5.2.3 Healthcare provider's ethical or legal proof of action 6 6 Trigger events 7 6.1 General Tell Tell STANDARD PREVIEW 7 6.2 Details of the event types and their contents 7 6.2.1 Access events to the personal health information 7 6.2.2 Query events to the personal health information 7 6.2.1 Access point to the personal health information 8 7.1 The general record formatog	2	Nori	native references	1	
5 Requirements and uses of audit data 5 5.1 Ethical and formal requirements 5 5.1.1 General 5 5.1.2 Access policy 5 5.1.3 Unambiguous identification of information system users 5 5.1.4 User roles 5 5.1.5 Secure audit records 6 5.2 Uses of audit data 6 5.2.1 Governance and supervision 6 5.2.2 Subjects of care exercising their rights 6 5.2.2 Subjects of care exercising their rights 6 5.2.2 Subjects of care exercising their rights 7 6.1 General Tell STANDARD PREVIEW 7 6.2 Details of the event types and their coptents 7 6.2 Details of the event types and their coptents 7 6.2.1 Access events to the personal health information 7 6.2.2 Query events to the personal health information 8 7.1 The general record format by standards sistabas 42db aca2 4236 8c90 8 7.	3	Tern	ns and definitions	1	
5 Requirements and uses of audit data 5 5.1 Ethical and formal requirements 5 5.1.1 General 5 5.1.2 Access policy 5 5.1.3 Unambiguous identification of information system users 5 5.1.4 User roles 5 5.1.5 Secure audit records 6 5.2 Uses of audit data 6 5.2.1 Governance and supervision 6 5.2.2 Subjects of care exercising their rights 6 5.2.2 Subjects of care exercising their rights 6 5.2.2 Subjects of care exercising their rights 7 6.1 General Tell STANDARD PREVIEW 7 6.2 Details of the event types and their coptents 7 6.2 Details of the event types and their coptents 7 6.2.1 Access events to the personal health information 7 6.2.2 Query events to the personal health information 8 7.1 The general record format by standards sistabas 42db aca2 4236 8c90 8 7.	4	Svm	bols and abbreviated terms	5	
5.1 Ethical and formal requirements 5 5.1.1 General 5 5.1.2 Access policy 5 5.1.4 User roles 5 5.1.5 Secure audit records 6 5.2.1 Uses of audit data 6 5.2.2 Subjects of care exercising their rights 6 5.2.3 Healthcare provider's ethical or legal proof of action 6 6 Trigger events 7 6.1 Generali Ten STANDARD PREVIEW 7 6.2 Details of the event types and their contents 7 6.2.1 Access events bot the personal health information 8 7.2 Query events to the personal health information 8 7.1 The general record formation standard information 9 7.1 Event ID 9 7.2.1 Event ID	5	-			
S.1.1 General S.1.2 Access policy S.1.2 Access policy S.1.3 Unambiguous identification of information system users S.1.5 Secure audit records S.1.5 Secure audit records S.1.5 Secure audit data S.2.1 Governance and supervision S.2.2 Subjects of care exercising their rights S.2.3 Healthcare provider's ethical or legal proof of action S.2.3 Healthcare provider's ethical or legal proof of action S.2.1 Governance and supervision S.2.2 Subjects of care exercising their rights S.2.3 Healthcare provider's ethical or legal proof of action S.2.2 Subjects of care exercising their rights S.2.3 Healthcare provider's ethical or legal proof of action S.2.2 Details of the event types and their contents S.2.2 Subjects of care exercising their rights S.2.2 S.2.2 Subjects of care exercising their rights S.2.2 S.2.2 Subjects of care exercising their rights S.2.2 S.2.2	3				
5.1.2 Access policy 5 5.1.3 Unambiguous identification of information system users 5 5.1.4 User roles 5 5.1.5 Secure audit records 6 6 5.2 Uses of audit data 6 6 5.2.1 Governance and supervision 6 5.2.2 Subjects of care exercising their rights 6 5.2.3 Subjects of care exercising their rights 6 5.2.3 Healthcare provider's ethical or legal proof of action 6 6 Trigger events 7 6.1 General Teh STANDARD PREVIEW 7 6.2 Details of the event types and their contents 7 6.2 Details of the event types and their contents 7 6.2.1 Access events to the personal health information 8 6.2.1 Access events to the personal health information 8 7 Audit record details SIST pren ISO 277892020 8 7.1 The general record formatics standards sistable 3424b-a6a2-4236-8c90 8 7.2 Trigger event identification 7 7 7 7 7 7 7 7 7		0.1			
5.1.3 Unambiguous identification of information system users 5 5.1.4 User roles 5 5.1.4 User roles 5 5.1.5 Secure audit records 6 6 5.2.1 Governance and supervision 6 5.2.2 Subjects of care exercising their rights 6 5.2.3 Healthcare provider's ethical or legal proof of action 6 6 Trigger events 7 6.2 Healthcare provider's ethical or legal proof of action 7 6.2 Details of the event types and their contents 7 6.2.1 Access events to the personal health information 7 6.2.1 Access events to the personal health information 7 6.2.1 Access events to the personal health information 8 7 Audit record details SIST prent ISO 27789-2020 8 7.1 The general record formatics standards sistaba842db-aca2-4236-8c90 8 7.2 Trigger event identification 7 7 7 7 7 7 7 7 7					
5.1.5 Secure audit records 6 5.2 Uses of audit data 6 5.2.1 Governance and supervision 6 5.2.2 Subjects of care exercising their rights 6 5.2.3 Healthcare provider's ethical or legal proof of action 6 6 Trigger events 7 6.1 Generali Tell STANDARD PREVIEW 7 6.2.1 Access events to fife personal dealth information 7 6.2.1 Access events to fife personal health information 8 7.2 Query events to the personal health information 8 7.2 The general record formatics standards standa			5.1.3 Unambiguous identification of information system users	5	
5.2 Uses of audit data 6 5.2.1 Governance and supervision 6 5.2.2 Subjects of care exercising their rights 6 5.2.3 Healthcare provider's ethical or legal proof of action 6 6 Trigger events 7 6.1 General Tech STANDARD PREVIEW 7 6.2 Details of the event types and their contents 7 6.2.1 Access events to the personal health information 8 6.2.1 Access events to the personal health information 7 6.2.2 Query events to the personal health information 8 7 Audit record details SIST DEALS DO 27789 2000 8 7.1 The general record format wastandards sist abs 42db-acc 4236-8c90 8 7.2 Trigger event identification 7/0sst-pen-so-27789-2020 9 7.2.1 Event ID 9 7.2.2 Event action code 10 7.2.3 Event date and time 10 7.2.4 Event outcome indicator 11 7.2.5 Event type code 11 <					
5.2.1 Governance and supervision 6 5.2.2 Subjects of care exercising their rights 6 5.2.3 Healthcare provider's ethical or legal proof of action 6 6 Trigger events 7 6.1 General Ten. STANDARD PREVIEW 7 6.2 Details of the event types and their contents 7 6.2.1 Access events to the personal health information 8 6.2.1 Access events to the personal health information 8 7.2 Query events to the personal health information 8 7.2 Trigger event identification SIST pren ISO 27789-2020 8 7.1 The general record format by standards sist ab342db-acc2 4236-8c90 8 7.2 Trigger event identification Code 10 7.2.1 Event D 9 7.2.2 Event action code 10 7.2.3 Event date and time 10 7.2.5 Event type code 11 7.3 User intrification 11 7.3.1 User intrification 12 7.3.2					
5.2.2 Subjects of care exercising their rights. 6 5.2.3 Healthcare provider's ethical or legal proof of action 6 6 Trigger events. 7 6.1 General Teh STANDARD PREVIEW 7 6.2 Details of the event types and their contents. 7 6.2.1 Access events to the personal health information 8 6.2.2 Query events to the personal health information 8 7 Audit record details. SIST prEN ISO 27789-2020 8 7.1 The general record formation standards/sist/abs/42fb-a6a2-4236-8c90- 8 7.2 Trigger event identification 7/osst-pren-sc-27789-2020 9 7.2.1 Event date and time. 10 7.2.2 Event action code. 10 7.2.3 Event date and time. 10 7.2.4 Event outcome indicator. 11 7.3.1 User identification. 11 7.3.2 Alternative user ID 12 7.3.3 User identification. 12 7.3.4 User is requestor. 12 <tr< td=""><td></td><td>5.2</td><td></td><td></td></tr<>		5.2			
6 Trigger events. 7 6.1 General Teh STANDARD PREVIEW 7 6.2 Details of the event types and their contents. 7 6.2.1 Access events to the personal field in information. 8 7.2.2 Query events to the personal health information. 8 7.1 The general record for imate standards six aba84.2db-a6a2.4236-8e90. 8 7.2 Trigger event identification 7/osist-pren-iso-27789-2020. 9 7.2.1 Event ID. 9 7.2.2 Event action code. 10 7.2.3 Event date and time. 10 7.2.4 Event outcome indicator. 11 7.3 User identification. 11 7.3.1 User ib ID. 11 7.3.2 Alternative user ID. 12 7.3.3 User is requestor. 12 7.3.4 User is requestor. 12 7.3.5 Role ID code. 12 7.3.6 Purpose of use. 13 7.4 Access point identification. 15			1		
6 Trigger events 7 6.1 General Teh STANDARD PREVIEW 7 6.2 Details of the event types and their contents 7 6.2.1 Access events to the personal health information 7 6.2.2 Query events to the personal health information 8 7 Audit record details oSIST nrN ISO 27789-2020 8 7.1 The general record formato's standards six abade 404-4642-4236-8690 8 7.2 Trigger event identification'//osst-pren-so-27789-2020 9 7.2.1 Event D 9 7.2.2 Event action code 10 7.2.2 Event date and time 10 7.2.4 Event outcome indicator 11 7.2.5 Event type code 11 7.3 User identification 11 7.3.1 User ibe indication 11 7.3.2 Alternative user ID 12 7.3.3 User is requestor 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12					
6.2.1 Access events to the personal health information 7 6.2.1 Access events to the personal health information 8 7 Audit record details OSIST prin ISO 27789-2020 8 7.1 The general record format by standards/sist/ab3842db-a6g2-4236-8c90 8 7.2 Trigger event identification //osist-pren-iso-27789-2020 9 7.2.1 Event ID 9 7.2.2 Event action code 10 7.2.3 Event date and time 10 7.2.4 Event outcome indicator 11 7.2.5 Event type code 11 7.3.1 User identification 11 7.3.2 Alternative user ID 12 7.3.3 User name 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5.1 Overview 15 7.5.2 Audit source identification 16 7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.5.5 Audit source type code 16	_		•		
6.2.1 Access events to the personal health information 7 6.2.1 Access events to the personal health information 8 7 Audit record details OSIST prin ISO 27789-2020 8 7.1 The general record format by standards/sist/ab3842db-a6g2-4236-8c90 8 7.2 Trigger event identification //osist-pren-iso-27789-2020 9 7.2.1 Event ID 9 7.2.2 Event action code 10 7.2.3 Event date and time 10 7.2.4 Event outcome indicator 11 7.2.5 Event type code 11 7.3.1 User identification 11 7.3.2 Alternative user ID 12 7.3.3 User name 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5.1 Overview 15 7.5.2 Audit source identification 16 7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.5.5 Audit source type code 16	6	Trigger events.			
6.2.1 Access events to the personal health information 7 6.2.2 Query events to the personal health information 8 7 Audit record details SIST prEN ISO 27789-2020 8 7.1 The general record formator standards/sis/ab3842db-a6a2-4236-8c90- 8 7.2 Trigger event identification 7/osst-pren-so-27789-2020 9 7.2.1 Event ID. 9 7.2.2 Event date and time 10 7.2.3 Event outcome indicator 11 7.3 User identification 11 7.3.1 User ibn 11 7.3.2 Alternative user ID 12 7.3.3 User is requestor 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.5.2 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3		6.1	Dotails of the event types and their contents		
6.2.2 Query events to the personal health information 8 Audit record details SIST prin ISO 27789-2020 7.1 The general record formatog standards/sis/ab3842db-a6a2-4236-8c90- 8 7.2 Trigger event identification / osst-pren-so-27789-2020 9 7.2.1 Event ID 9 7.2.2 Event action code 10 7.2.3 Event date and time 10 7.2.4 Event outcome indicator 11 7.2.5 Event type code 11 7.3 User identification 11 7.3.1 User ID 11 7.3.2 Alternative user ID 12 7.3.3 User name 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.5.2 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source type code 16 7.6.1 Overview 17 7.6.2 Participant object identification 17 7.6.3 Participant object type		0.2	6.2.1 Access events to the personal health information	7	
7 Audit record details OSIST prEN ISO 27789-2020 8 7.1 The general record format of standards/sist/ab3842db-a6a2-4236-8c90 8 7.2 Trigger event identification Vosist-pren-iso-27789-2020 9 7.2.1 Event ID 9 7.2.2 Event action code 10 7.2.3 Event date and time 10 7.2.4 Event outcome indicator 11 7.2.5 Event type code 11 7.3 User identification 11 7.3.1 User ID 11 7.3.2 Alternative user ID 12 7.3.3 User aname 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.5.2 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit source type code <td< td=""><td></td><td></td><td>6.2.2 Ouery events to the personal health information</td><td>8</td></td<>			6.2.2 Ouery events to the personal health information	8	
7.2.1 Event ID 9 7.2.2 Event action code 10 7.2.3 Event date and time 10 7.2.4 Event outcome indicator 11 7.2.5 Event type code 11 7.3 User identification 11 7.3.1 User ID 11 7.3.2 Alternative user ID 12 7.3.3 User name 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source type code 16 7.5.4 Audit source type code 16 7.6.6 Participant object identification 17 7.6.1 Overview 17 7.6.2 Participant object type code 18 7.6.4 Participant object type code role 18 7.6.5 Participant object tolet data life cycle 20	7	A d :			
7.2.1 Event ID 9 7.2.2 Event action code 10 7.2.3 Event date and time 10 7.2.4 Event outcome indicator 11 7.2.5 Event type code 11 7.3 User identification 11 7.3.1 User ID 11 7.3.2 Alternative user ID 12 7.3.3 User name 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source type code 16 7.5.4 Audit source type code 16 7.6.6 Participant object identification 17 7.6.1 Overview 17 7.6.2 Participant object type code 18 7.6.4 Participant object type code role 18 7.6.5 Participant object tolet data life cycle 20	/	7.1 The attacks all substantial of the attack of the attac			
7.2.1 Event ID 9 7.2.2 Event action code 10 7.2.3 Event date and time 10 7.2.4 Event outcome indicator 11 7.2.5 Event type code 11 7.3 User identification 11 7.3.1 User ID 11 7.3.2 Alternative user ID 12 7.3.3 User name 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source type code 16 7.5.4 Audit source type code 16 7.6.6 Participant object identification 17 7.6.1 Overview 17 7.6.2 Participant object type code 18 7.6.4 Participant object type code role 18 7.6.5 Participant object tolet data life cycle 20		7.1	Trigger event identification 7/osist-pren-iso-27789-2020	9	
7.2.2 Event action code 10 7.2.3 Event date and time 10 7.2.4 Event outcome indicator 11 7.2.5 Event type code 11 7.3.1 User identification 11 7.3.1 User ID 11 7.3.2 Alternative user ID 12 7.3.3 User name 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source type code 16 7.5.4 Audit source type code 16 7.5.2 Participant object identification 17 7.6.1 Overview 17 7.6.2 Participant object type code 18 <td></td> <td>7.2</td> <td>7.2.1 Event ID.</td> <td>9</td>		7.2	7.2.1 Event ID.	9	
7.2.4 Event outcome indicator 11 7.2.5 Event type code 11 7.3 User identification 11 7.3.1 User ID 11 7.3.2 Alternative user ID 12 7.3.3 User name 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5.1 Overview 15 7.5.2 Audit source identification 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source type code 16 7.5.4 Audit source type code 16 7.6.1 Overview 17 7.6.2 Participant object type code 18 7.6.3 Participant object type code role 18 7.6.4 Participant object type code role 18 7.6.5 Participant object ID ty					
7.2.5 Event type code 11 7.3 User identification 11 7.3.1 User ID 11 7.3.2 Alternative user ID 12 7.3.3 User name 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.5.4 Audit source type code 16 7.6.1 Overview 17 7.6.2 Participant object identification 17 7.6.2 Participant object type code 18 7.6.3 Participant object type code role 18 7.6.4 Participant object data life cycle			7.2.3 Event date and time	10	
7.3 User identification 11 7.3.1 User ID 11 7.3.2 Alternative user ID 12 7.3.3 User name 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.5.4 Audit source type code 16 7.5.4 Participant object identification 17 7.6.1 Overview 17 7.6.2 Participant object type code 18 7.6.3 Participant object type code role 18 7.6.4 Participant object data life cycle 19 7.6.5 Participant obj					
7.3.1 User ID 11 7.3.2 Alternative user ID 12 7.3.3 User name 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.5.4 Audit source type code 16 7.6.1 Overview 17 7.6.2 Participant object identification 17 7.6.2 Participant object type code 18 7.6.3 Participant object type code role 18 7.6.4 Participant object data life cycle 19 7.6.5 Participant object ID type code 20		7 0			
7.3.2 Alternative user ID 12 7.3.3 User name 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.6 Participant object identification 17 7.6.1 Overview 17 7.6.2 Participant object type code 18 7.6.3 Participant object type code role 18 7.6.4 Participant object data life cycle 19 7.6.5 Participant object ID type code 20		7.3			
7.3.3 User name 12 7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.6 Participant object identification 17 7.6.1 Overview 17 7.6.2 Participant object type code 18 7.6.3 Participant object type code role 18 7.6.4 Participant object data life cycle 19 7.6.5 Participant object ID type code 20					
7.3.4 User is requestor 12 7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.6.1 Overview 17 7.6.2 Participant object identification 17 7.6.2 Participant object type code 18 7.6.3 Participant object type code role 18 7.6.4 Participant object data life cycle 19 7.6.5 Participant object ID type code 20					
7.3.5 Role ID code 12 7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.5.4 Audit source type code 16 7.6.1 Overview 17 7.6.2 Participant object identification 17 7.6.2 Participant object type code 18 7.6.3 Participant object type code role 18 7.6.4 Participant object data life cycle 19 7.6.5 Participant object ID type code 20					
7.3.6 Purpose of use 13 7.4 Access point identification 15 7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.5.4 Audit source type code 16 7.6.1 Overview 17 7.6.2 Participant object type code 18 7.6.3 Participant object type code role 18 7.6.4 Participant object data life cycle 19 7.6.5 Participant object ID type code 20			•		
7.4.1 Network access point type code 15 7.4.2 Network access point ID 15 7.5 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.6 Participant object identification 17 7.6.1 Overview 17 7.6.2 Participant object type code 18 7.6.3 Participant object type code role 18 7.6.4 Participant object data life cycle 19 7.6.5 Participant object ID type code 20					
7.4.2 Network access point ID 15 7.5 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.6 Participant object identification 17 7.6.1 Overview 17 7.6.2 Participant object type code 18 7.6.3 Participant object type code role 18 7.6.4 Participant object data life cycle 19 7.6.5 Participant object ID type code 20		7.4			
7.5 Audit source identification 15 7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.6 Participant object identification 17 7.6.1 Overview 17 7.6.2 Participant object type code 18 7.6.3 Participant object type code role 18 7.6.4 Participant object data life cycle 19 7.6.5 Participant object ID type code 20			· · · · · · · · · · · · · · · · · · ·		
7.5.1 Overview 15 7.5.2 Audit enterprise site ID 16 7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.6 Participant object identification 17 7.6.1 Overview 17 7.6.2 Participant object type code 18 7.6.3 Participant object type code role 18 7.6.4 Participant object data life cycle 19 7.6.5 Participant object ID type code 20		7.5	1		
7.5.2 Audit enterprise site ID 16 7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.6 Participant object identification 17 7.6.1 Overview 17 7.6.2 Participant object type code 18 7.6.3 Participant object type code role 18 7.6.4 Participant object data life cycle 19 7.6.5 Participant object ID type code 20		7.5			
7.5.3 Audit source ID 16 7.5.4 Audit source type code 16 7.6 Participant object identification 17 7.6.1 Overview 17 7.6.2 Participant object type code 18 7.6.3 Participant object type code role 18 7.6.4 Participant object data life cycle 19 7.6.5 Participant object ID type code 20					
7.5.4 Audit source type code			1		
7.6 Participant object identification					
7.6.1 Overview		7.6			
7.6.3 Participant object type code role 18 7.6.4 Participant object data life cycle 19 7.6.5 Participant object ID type code 20			7.6.1 Overview	17	
7.6.4 Participant object data life cycle			1 , 11		
7.6.5 Participant object ID type code20					

oSIST prEN ISO 27789:2020

ISO/DIS 27789:2020(E)

		7.6.7	Participant object sensitivity	21
		7.6.8	Participant object ID	21
		7.6.9	Participant object name	21
		7.6.10	Participant object query	21
		7.6.11	Participant object sensitivity Participant object ID Participant object name Participant object query Participant object detail	22
8	Audit records for individual events			22
	8.1	Access	events	22
	8.2	Query	events	24
9	Secure management of audit data 9.1 Security considerations			26
	9.1	Securit	ty considerations	26
	9.2	Securir	ng the availability of the audit systemion requirements	26
	9.3	Retenti	ion requirements	26
	9.4	Securir	ng the confidentiality and integrity of audit trails	26
	9.5	Access	to audit data	27
Annex	28			
Annex B (informative) Audit log services				
Biblio	granh	V		43

iTeh STANDARD PREVIEW (standards.iteh.ai)

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 27789 was prepared by Technical Committee ISO/TC 215, Health informatics,.

This second edition cancels and replaces the first edition (ISO/TS 27789:2013), which has been technically revised.

The main changes compared to the previous edition are as follows: EW

- update ISO27799 chapter titles to the latest S.iteh.ai)
- match between audit record format and DICOM format
- review the content of Annex A audit scenarios 816cb761b507/osist-pren-iso-27789-2020
- review the chart of <u>Annex B</u> audit log services
- update bibliography.

Introduction

0.1 General

Personal health information is regarded by many as among the most confidential of all types of personal information and protecting its confidentiality is essential if the privacy of subjects of care is to be maintained. In order to protect the consistency of health information, it is also important that its entire life cycle be fully auditable. Health records should be created, processed and managed in ways that guarantee the integrity and confidentiality of their contents and that support legitimate control by subjects of care in how the records are created, used and maintained.

Trust in electronic health records requires physical and technical security elements along with data integrity elements. Among the most important of all security requirements to protect personal health information and the integrity of records are those relating to audit and logging. These help to ensure accountability for subjects of care who entrust their information to electronic health record (EHR) systems. They also help to protect record integrity, as they provide a strong incentive to users of such systems to conform to organizational policies on the use of these systems.

Effective audit and logging can help to uncover misuse of EHR systems or EHR data and can help organisations and subjects of care obtain redress against users abusing their access privileges. For auditing to be effective, it is necessary that audit trails contain sufficient information to address a wide variety of circumstances (see Annex A).

Audit logs are complementary to access controls. The audit logs provide a means to assess compliance with organizational access policy and can contribute to improving and refining the policy itself. But as such a policy has to anticipate the occurrence of unforeseen or emergency cases, analysis of the audit logs becomes the primary means of ensuring access control for those cases.

This document is strictly limited in scope to logging of events. Changes to data values in fields of an EHR are presumed to be recorded in the EHR database system itself and not in the audit log. It is presumed that the EHR system itself contains both the previous and updated values of every field. This is consistent with contemporary point-in-time database architectures. The audit log itself is presumed to contain no personal health information other than identifiers and links to the record.

Electronic health records on an individual person may reside in many different information systems within and across organisational or even jurisdictional boundaries. To keep track of all actions that involve records on a particular subject of care, a common framework is a prerequisite. This document provides such a framework. To support audit trails across distinct domains it is essential to include references in this framework to the policies that specify the requirements within the domain, such as access control rules and retention periods. Domain policies may be referenced implicitly by identification of the audit log source.

0.2 Benefits of using this document

Standardization of audit trails on access to electronic health records aims at two goals:

- ensuring that information captured in an audit log is sufficient to clearly reconstruct a detailed chronology of the events that have shaped the content of an electronic health record, and
- ensuring that an audit trail of actions relating to a subject of care's record can be reliably followed, even across organizational domains.

This document is intended for those responsible for overseeing health information security or privacy and for healthcare organizations and other custodians of health information seeking guidance on audit trails, together with their security advisors, consultants, auditors, vendors and third-party service providers.

0.3 Comparison with related standards on electronic health record audit trails

This document conforms to the requirements of ISO 27799, *Health informatics* — *Security management in health using ISO/IEC 27002*, insofar as they relate to auditing and audit trails.

Some readers may be familiar with Internet Engineering Task Force (IETF) Request for Comment (RFC) 3881 Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications. ^[13] (Readers not already familiar with IETF RFC 3881 need not refer to that document, as familiarity with it is not required to understand this document). Informational RFC 3881, dated 2004-09 and no longer listed as active in the IETF database, was an early and useful attempt at specifying the content of audit logs for healthcare. To the extent possible, this document builds upon, and is consistent with, the work begun in RFC 3881 with respect to access to the EHR.

0.4 A note on terminology

Several closely related terms are defined in <u>Clause 3</u> (Terms and definitions). An *audit log* is a chronological sequence of *audit records*; each audit record contains evidence of directly pertaining to and resulting from the execution of a process or system function. As EHR systems can be complex aggregations of systems and databases, there may be more than one audit log containing information on system events that have altered a subject of care's EHR. Although the terms *audit trail* and *audit log* are often used interchangeably, in this document the term *audit trail* refers to the collection of all audit records from one or more audit logs that refer to a specific subject of care or specific electronic health record or specific user. An *audit system* provides all the information processing functions necessary to maintain one or more audit logs TANDARD PREVIEW

(standards.iteh.ai)

oSIST prEN ISO 27789:2020

iTeh STANDARD PREVIEW (standards.iteh.ai)

Health informatics — Audit trails for electronic health records

1 Scope

This document specifies a common framework for audit trails for electronic health records (EHR), in terms of audit trigger events and audit data, to keep the complete set of personal health information auditable across information systems and domains.

It is applicable to systems processing personal health information which, complying with ISO 27799, create a secure audit record each time a user accesses, creates, updates, or archives personal health information via the system.

NOTE Such audit records at minimum uniquely identify the user, uniquely identify the subject of care, identify the function performed by the user (record creation, access, update, etc.), and record the date and time at which the function was performed.

This document covers only actions performed on the EHR, which are governed by the access policy for the domain where the electronic health record resides. It does not deal with any personal health information from the electronic health record, other than identifiers, the audit record only containing links to EHR segments as defined by the governing access policy.

It does not cover the specification and use of audit logs for system management and system security purposes, such as the detection of performance problems, application flaw, or support for a reconstruction of data, which are dealt with by general computer security standards such as ISO/IEC 15408[9].

OSIST pren ISO 27789 2020

https://standards.iteh.ai/catalog/standards/sist/ab3842db-a6a2-4236-8c90-

Annex A gives examples of audit scenarios. Annex B gives an overview of audit log services.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 27799:2016, Health informatics — Information security management in health using ISO/IEC 27002

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at http://www.electropedia.org/

3.1

access control

means to ensure that access to assets is authorized and restricted based on business and security requirements

[SOURCE: ISO/IEC 27000:2009, definition 2.1]

3.2

access policy

definition of the obligations for authorizing access to a resource

3.3

accountability

principle that individuals, organizations, and the community are responsible for their actions and may be required to explain them to others

[SOURCE: ISO 15489-1:2001, definition 3.2]

3.4

audit

systematic and independent examination of accesses, additions, or alterations to electronic health records to determine whether the activities were conducted, and the data were collected, used, retained or disclosed according to organizational standard operating procedures, policies, good clinical practice, and applicable regulatory requirement(s).

3.5

audit archive

archival collection of one or more audit logs

3.6

audit data

data obtained from one or more audit records

3.7

iTeh STANDARD PREVIEW

audit log (standards.iteh.ai) chronological sequence of audit records, each of which contains data about a specific event

O

oSIST prEN ISO 27789:2020

audit record

https://standards.iteh.ai/catalog/standards/sist/ab3842db-a6a2-4236-8c90-

record of a single specific event in the life cycle of an electronic health record

3.9

3.8

audit system

information processing system that maintains one or more audit logs

3.10

audit trail

collection of audit records from one or more audit logs relating to a specific subject of care or a specific electronic health record

3.11

authentication

provision of assurance that a claimed characteristic of an entity is correct

[SOURCE: ISO/IEC 27000:2009, definition 2.5]

3.12

authorization

granting of privileges, which includes the granting of privileges to access data and functions

Note 1 to entry: derived from ISO 7498-2: the granting of rights, which includes the granting of access based on access rights

3.13

authority

entity responsible for issuing certificates

3.14

availability

property of being accessible and useable upon demand by an authorized entity

[SOURCE: ISO/IEC 27000:2009, definition 2.7]

3.15

confidentiality

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO/IEC 27000:2009, definition 2.9]

3.16

Coordinated Universal Time

UTC

time scale which format the basis of a coordinated radio dissemination of standard frequencies and time signals; it corresponds exactly in rate with international atomic time, but differs from it by an integral number of seconds

[SOURCE: IEC 60050-713:1998]

3.17

data integrity

property that data have not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 7498-2:1989, definition 3.3.21] ARD PREVIEW

3.18

(standards.iteh.ai)

electronic health record

EHR

oSIST prEN ISO 27789:2020

comprehensive, structured set of clinical demographics environmental social, and financial data in electronic form, documenting the health caregiven to a single individual

[SOURCE: ASTM E 1769:1995]

3.19

EHR segment

part of an EHR that constitutes a distinct resource for the access policy

3.20

identification

performance of tests to enable a data processing system to recognize entities

[SOURCE: ISO/IEC 2382-8:1998, definition 08.04.12 (as identity authentication, identity validation)]

3.21

identifier

piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

3.22

information security

preservation of confidentiality, integrity and availability of information

[SOURCE: ISO/IEC 27000:2009, definition 2.19]

3.23

integrity

property of protecting the accuracy and completeness of assets

[SOURCE: ISO/IEC 27000:2009, definition 2.25]

3.24

object identifier

OID

globally unique identifier for an information object

Note 1 to entry: The object identifiers used in this document refer to code systems. These code systems may be defined in a standard or locally defined per implementation. The object identifier is specified using the Abstract Syntax Notation One (ASN.1) defined in ISO/IEC 8824-1 and ISO/IEC 8824-2.

3.25

policy

set of legal, political, organizational, functional and technical obligations for communication and cooperation

[SOURCE: ISO/TS 22600-1:2006, definition 2.22]

3.26

privilege

capacity assigned to an entity by an authority

3.27

records management

field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records

[SOURCE: ISO 15489-1, definition 3.16] STANDARD PREVIEW

3.28

(standards.iteh.ai)

role

set of competences and/or performances associated with artask 020

3.29

https://standards.iteh.ai/catalog/standards/sist/ab3842db-a6a2-4236-8c90-

8f6cb761b507/osist-pren-iso-27789-2020

sensitivity

measure of the potential or perceived potential to create harm to a data subject, or to be abused, or misused

3.30

security policy

plan or course of action adopted for providing computer security

[SOURCE: ISO/IEC 2382-8:1998, definition 08.01.06]

3.31

subject of care

person scheduled to receive, receiving, or having received a health service

[SOURCE: ISO 18308:2011, definition 3.47]

3.32

user

person, device, or program that uses an EHR system for data processing or health information exchange.

4 Symbols and abbreviated terms

EHR Electronic Health Record

HL7 Health Level Seven International

OID Object Identifier

UTC Coordinated Universal Time

5 Requirements and uses of audit data

5.1 Ethical and formal requirements

5.1.1 General

Health care providers have their professional ethical responsibilities to meet. Among these are protecting the privacy of subjects of care and documenting the findings and activities of care. Restricting access to health records and ensuring their appropriate use are both essential requirements in health care and in many jurisdictions these requirements are set down in law.

Secure audit trails of access to electronic health records may support compliance with professional ethics, organizational policies and legislation, but they are not sufficient in themselves to assess completeness of an electronic health record. A R D PREVIEW

5.1.2 Access policy (standards.iteh.ai)

An organization responsible for the maintaining an audit 10g shall identify the access policy governing all accesses logged. https://standards.iteh.ai/catalog/standards/sist/ab3842db-a6a2-4236-8c90-

The access policy shall be in accordance with ISO 27799, 9.1.1 Access control policy.

NOTE 1 The access policy is presumed to define an EHR segment structure.

NOTE 2 In the audit record the access policy is identified by the audit log source.

Guidance on specifying and implementing access policies can be found in ISO 22600.^[6] A field "Participant object Permission PolicySet" is defined in <u>clause 7.6.6</u> to support referencing the actual policies in the audit record.

5.1.3 Unambiguous identification of information system users

The audit trails shall provide sufficient data to unambiguously identify all authorized health information system users. Users of the information system can be persons, but also other entities.

The audit trails shall provide sufficient data to determine which authorized users and external systems have accessed or been sent health record data from the system.

5.1.4 User roles

The audit trail shall show the role of the user while performing the recorded action on personal health information.

Information systems processing personal health information should support role-based access control capable of mapping each user to one or more roles, and each role to one or more system functions, as recommended in ISO 27799, 9.2.3 *Management of privileged access rights*.

Functional and structural roles are documented in ISO/TS 21298.[4] Additional guidance on privilege management in health is given by ISO/TS 22600, parts 1-3[6].