

DIN EN ISO 27789:2022-01 (E)

Health informatics - Audit trails for electronic health records (ISO 27789:2021); English version EN ISO 27789:2021

Contents	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 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.....	6
5.1.4 User roles	6
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.....	7
5.2.3 Evidence and retention requirements	7
6 Trigger events	7
6.1 General.....	7
6.2 Details of the event types and their contents	8
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	8
7.1 The general record format.....	8
7.2 Trigger event identification.....	10
7.2.1 Event ID	10
7.2.2 Event action code	11
7.2.3 Event date and time	11
7.2.4 Event outcome indicator.....	12
7.2.5 Event type code	12
7.3 User identification	12
7.3.1 User ID	12
7.3.2 Alternative user ID	13
7.3.3 User name.....	13
7.3.4 User is requestor	13
7.3.5 Role ID code	13
7.3.6 Purpose of use	14
7.4 Access point identification.....	15
7.4.1 Network access point type code.....	15
7.4.2 Network access point ID	16
7.5 Audit source identification	16
7.5.1 Overview	16
7.5.2 Audit enterprise site ID	17
7.5.3 Audit source ID.....	17
7.5.4 Audit source type code	17

7.6	Participant object identification.....	18
7.6.1	Overview	18
7.6.2	Participant object type code.....	19
7.6.3	Participant object type code role	19
7.6.4	Participant object data life cycle and record entry lifecycle events	20
7.6.5	Participant object ID type code.....	22
7.6.6	Participant object Permission PolicySet	23
7.6.7	Participant object sensitivity.....	23
7.6.8	Participant object ID	24
7.6.9	Participant object name.....	24
7.6.10	Participant object query	24
7.6.11	Participant object detail, Participant object description	24
8	Audit records for individual events.....	25
8.1	Access events	25
8.2	Query events.....	26
9	Secure management of audit data	28
9.1	Security considerations.....	28
9.2	Securing the availability of the audit system	28
9.3	Retention requirements.....	29
9.4	Securing the confidentiality and integrity of audit trails	29
9.5	Access to audit data.....	29
	Annex A (informative) Audit scenarios.....	30
	Annex B (informative) Audit log services.....	36
	Bibliography.....	45