TECHNICAL SPECIFICATION

ISO/TS 21547

First edition
2010-02-15

Health informatics — Security requirements for archiving of electronic health records — Principles

Informatique de santé — Exigences de sécurité pour l'archivage des dossiers de santé électroniques — Principes

Reference number
ISO/TS 21547:2010(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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.

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.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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/TS 21547 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Introduction

The healthcare industry is faced with the challenge of reducing costs by moving from paper-based processes to automated electronic processes. New models of healthcare delivery emphasise the need for patient information to be shared among a growing number of specialist healthcare providers and across traditional organizational boundaries.

Paper-based patient records have traditionally been stored in archives which were once located near work sites; however, it is now common that these documents are located in the organization's centralized archive. Due to lack of space or to ensure safekeeping, paper data from archives have been transferred to microfilm.

When patient data are transferred to an electronic format, data are either maintained in a simple database or on paper printouts in an archive. During the past few years, electronic archives independent of basic systems have been created, such as DICOM – a standard archival system for medical images. An electronic archive can become a shared information storage system, an archive containing different software and even different organizations. Centralized administration provides opportunities for managing good data security and utilization of archival information in accordance with the patient's requests.

Electronic data storage is threatened by the same basic hazards as paper storage. Data can disappear or the ability to read and understand it can be lost. Electronic media such as magnetic tapes, diskettes and hard disks can break, be destroyed or get lost. We only have a few decades of experience as to their durability. Merely retaining the media does not guarantee that the data will be available. As computer hardware and software are quickly upgraded, older, yet still-functioning media cannot be used with current readers or software because they are no longer able to read the stored data. With the development of technology, we must be prepared to transfer old data to new media whenever necessary. Data structures must also be converted or else unstructured data must be used.

Issues of stability and integrity threaten the storage of electronic data more than paper-based data. The unlawful usurping or copying of data must also be effectively prevented.

Electronic patient records must be available throughout their whole lifecycle. The need to access patient records regardless of place and time has increased data transfer between service provider organizations and healthcare professionals within the last few years. Particularly, data transfer involving different software has greatly increased over the past few years. The objective to reinforce patient rights to self-determination and participation in healthcare at its different stages invites the opportunity for the patient to gain more information concerning his or her care.

An EHR-archive (web-based, regionally centralized or organization-specifically distributed) can manage the aforementioned data usage and transfer needs in a cost-effective and information-secure way. The use of health services across national borders is continuously increasing due to mobility of inhabitants, internationalization of companies and virtualization of health services. In cases where the EHR-archive discloses records over borderlines, it is necessary that the archive be trusted.

The healthcare environment is unique. Any information system planned for use in this domain should understand healthcare-specific features such as:

— specific ethical and legal environments;

— in cases where personal health information is accessed, used or disclosed, privacy protection should be taken into account;

— strong regulations for who can access or disclose healthcare records, when and for what purpose;

— in many countries, citizens/patients have the right to control the use or disclosure of their records using opt-out and/or consent methods;

— citizens/patients can have the right to know who has used their electronic health records (EHRs) and for what purpose;

— health service providers or service provider organizations have the responsibility for managing the records;

— EHRs have a very long preservation time;

— EHR content is sensitive and has specific context and purpose;

— EHR content can grow (e.g. be dynamic) during the preservation time;

— specific responsibilities for EHR management or use;

— the information content of the EHR has context, purpose and sensitivity based access and disclosure rules;

— the nature of the EHR or its parts can change during the preservation time;

— EHR content should be understandable during the whole preservation time;

— for confidentiality and legal purposes, it might be necessary to prove the non-repudiation of events occurring during the preservation time of the EHR.

Not all of the above-mentioned features are unique for healthcare. Features described are common for most countries in the world, but there are also variations depending on national regulatory and normative environments. In any case, it is clear that healthcare forms a unique environment for records management and archiving.

Digital archiving is not a healthcare-specific question. Digital libraries and many other organizations are developing both the necessary technology and the requirements for digital archiving. However, based on the unique nature of healthcare information, the following healthcare-specific questions remain to be solved:

a) health information has a very long preservation time (up to 100+ years);

b) the content (e.g. data objects/documents) of the EHR can be dynamic during its lifetime (e.g. the service provider can add new fixed parts to the record before it is sent to the eArchive);

c) data content is sensitive;

d) a high degree of security, confidentiality and privacy protection is required;

e) there is a strong legal framework regulating who can access, what and when;

f) data objects have context, purpose and sensitivity based access/disclosure rules;

g) the nature of data can be legal for a given period;

h) non-repudiation of data and evidence should be secured during the whole preservation time.

Standards already exist for long-term preservation of digital documents. For example ISO 14721 defines a reference model for open archival information systems (OAIS). The ISO 15489 series, clearly shows how any organization can systematically and effectively improve their record-keeping. ISO 19005-1 defines a standard file format for preservation.

Many countries have already developed frameworks or “codes of practice” for preservation of health records (Annexes B to F). It is possible, based on already existing standards and national frameworks, to develop an international standard and guidelines, setting requirements for the secure archiving of electronic health records.

Health informatics — Security requirements for archiving of electronic health records — Principles

IMPORTANT — The electronic file of this document contains colours which are considered to be useful for the correct understanding of the document. Users should therefore consider printing this document using a colour printer.

1 Scope

The purpose of this Technical Specification is to define the basic principles needed to securely preserve health records in any format for the long term. It concentrates on previously documented healthcare-specific archiving problems. It also gives a brief introduction to general archiving principles. Unlike the traditional approach to standardization work, where the perspective is that of modelling, code sets and messages, this Technical Specification looks at archiving from the angle of document management and related privacy protection. The document management angle has traditionally been used in connection with patient records in paper form and it can also be applied to digitally stored documents. There are different architectural and technical ways to develop and implement long-term preservation of electronic health records. Archiving can be a function of the online record-keeping system, and we can have a separate independent archive or a federated one. Electronic health records are, in many cases, archived in the form of documents, but other technical solutions also exist.

In this Technical Specification archiving is understood to be a wider process than just the permanent preservation of selected records. Archiving of EHRs is a holistic process covering records maintenance, retention, disclosure and destruction when the record is not in active use. Archiving also includes tasks the EHR system should perform before the record is sent to the EHR-archive.

This Technical Specification defines architecture and technology-independent security requirements for the long-term preservation of EHRs having fixed content.

This Technical Specification and a complementary Technical Report, ISO/TR 21548, concentrate on the security requirements (integrity, confidentiality, availability and accountability) necessary for ensuring adequate protection of health information in long-term digital preservation. This Technical Specification will also address privacy protection requirements for both the EHR and eArchiving systems used in the healthcare environment.

This Technical Specification defines functional security requirements for long-term archiving of EHRs, but the practical archiving models and technology required are outside the concept of this Technical Specification.

It is also outside of the Scope of this Technical Specification to comment on the following.

— The creation, management and storage of active health records (records which can be modified, updated and accessed any time at the level of a single object or item) inside the EHR-system. However this Technical Specification defines responsibilities and tasks the EHR-system should undertake before it transfers an EHR to the electronic archive.

— The content of information submission packets sent to the EHR-archive. However this Technical Specification defines security requirements for those packets.

— Any storage structures used (such as DICOM, HL7 or XML) or metafile descriptions used (such as Dublin core or HL7 CDA header) in the eArchiving process.

— Implementation of security services such as PKI, electronic signatures, etc.

— Any of the storage times of EHRs or media applicable for their storage; rather, these will continue to be provided in accordance with national legislation.

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/IEC 13888 (all parts), *Information technology — Security techniques — Non-repudiation*

ISO 14721, *Space data and information transfer systems — Open archival information system — Reference model*

ISO 15489-1, *Information and documentation — Records management — Part 1: General*

ISO/TR 15489-2, *Information and documentation — Records management — Part 2: Guidelines*

ISO/IEC 17799, *Information technology — Security techniques — Code of practice for information security management*

ISO/TS 18308, *Health informatics — Requirements for an electronic health record architecture*

ISO/TR 18492, *Long-term preservation of electronic document-based information*

ISO/TR 21548, *Health informatics — Security requirements for archiving of electronic health records — Guidelines*

ISO/TS 22600-1, *Health informatics — Privilege management and access control — Part 1: Overview and policy management*

ISO/TS 22600-2, *Health informatics — Privilege management and access control — Part 2: Formal models*

ISO 23081-1, *Information and documentation — Records management processes — Metadata for records — Part 1: Principles*

ISO 27799, *Health informatics — information security management in health using ISO/IEC 27002*

EN 13606 (all parts), *Health informatics — Electronic health record communication*

3 Terms and definitions

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

3.1 General terms

3.1.1
application
any software process used in healthcare information systems, including those without any direct role in treatment or diagnosis

NOTE In some jurisdictions, software processes can be regulated medical devices.

3.1.2
archive
organization that intends to preserve information for access and use for any designed users or process

NOTE Adapted from OAIS Red Book, June 12, 2001. Electronic archive (EHR-archive) preserves information in digital format. It is an information system that manages and provides access to records through their whole lifecycle. EHR-archive is an archive preserving digitalized health records.

3.1.3
archiving process
holistic long-term preservation process covering the whole lifecycle of the health record

3.1.4
administration
archival entity that contains the services and functions needed to control the operation of functional entities on a day-to-day basis

3.1.5
content information
set of information that is the original target for preserving

3.1.6
data
re-interpretable representation of information in a formalized manner suitable for communication, interpretation or processing

3.1.7
digital preservation
storage, maintenance, and access to a digital object over a long time, usually as a consequence of applying one or more preservation strategies

NOTE 1 Adapted from ELAG[1)] 2001.

NOTE 2 Preservation consists of processes and operations involved in ensuring the technical and intellectual survival of authentic records through time (see ISO 15489-1).

3.1.8
directory
organizational unit or container, used to organize folders and files into a hierarchical structure

3.1.9
eArchiving process
holistic long-term preservation process covering the whole lifecycle of the electronic health record (EHR)

3.1.10
EHR
comprehensive, structured set of clinical, demographic, environmental, social and financial data and information in electronic form, documenting the healthcare given to a single individual

NOTE Adapted from ASTM E1769.

3.1.11
EHR-archive
EHR-archive that preserves fixed EHRs for a long time

3.1.12
EHR-system
set of components that forms the mechanism from which patients, records are created, used, stored and retrieved.

NOTE 1 It includes people, data, rules and procedures, processing and storage of data, and communication facilities.

NOTE 2 A narrow definition says that the EHR-system is a system for recording, retrieving, and manipulating information in electronic healthcare records. See EN 13606.

1) European Library Automation Group.

3.1.13
fixity
permanent character or condition

NOTE Fixity information is that which documents mechanisms to ensure that the Content Information object has not been altered in an undocumented manner. See ISO 14721.

3.1.14
healthcare organization
officially registered organization that has a main activity related to healthcare services or health promotion

NOTE 1 Examples include hospitals, internet healthcare website providers and healthcare research institutions.

NOTE 2 The organization should be recognised as legally liable for its activities but need not be registered for its specific role in health. An internal part of an organization is called here an organizational unit as in X.501.

3.1.15
health professional
person who is authorized by a nationally recognised body, to be qualified to perform certain health services

NOTE 1 The types of registering or accrediting bodies differ by country and profession. Nationally recognised bodies include local or regional governmental agencies, independent professional associations and other formally and nationally recognised organizations. They can be exclusive or non-exclusive in their territory.

NOTE 2 A nationally recognised body in this definition does not imply one nationally controlled system of professional registration but in order to facilitate international communication it would be preferable that one nationwide directory of recognised health professional registration bodies exists.

EXAMPLE Physicians, registered nurses and pharmacists.

3.1.16
information
any type of knowledge that can be exchanged

3.1.17
long-term preservation
act of maintaining information in a correct and independently understandable form over a long time

3.1.18
metadata
data describing context, content and structure of records and their management through time

ISO 15489-1:2001, definition 3.12.

3.1.19
patient/consumer
person who is the receiver of health-related services and an actor in a health information system

3.1.20
privacy
freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual

ISO/IEC 2382-8:1998, definition 08.01.23.

3.1.21
privacy protection
implementation of appropriate safeguards to ensure the security and confidentiality of data records, as well as to protect the records against threats or hazards that could result in substantial embarrassment, harm, inconvenience or unfairness to any person

3.1.22
privacy policy
privacy protection policy
document that states, in writing, principles of data protection used by an organization

NOTE It can be national as is the NHS Care Record Guarantee or local, made by an organization.

3.1.23
records management
field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records

NOTE Adapted from the NHS Code of Practice.

3.1.24
record-keeping system
information system that captures, manages and provides access to records through time

NOTE 1 Adapted from the NHS Code of Practice.

NOTE 2 The EHR-system is a typical record-keeping system.

3.1.25
reference information
information that provides identifiers that allow an outside system to refer unambiguously to the particular information

3.1.26
replication
digital duplication where there is no change to the information

3.1.27
structure information
information that imports knowledge about how other information is organized

3.2 Security services terms

3.2.1
access control
means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways

ISO/IEC 2382-8:1998, definition 08.04.01.

3.2.2
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

ISO 7498-2:1989, definition 3.3.3.

3.2.3
asymmetric cryptographic algorithm
algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ

ISO/IEC 10181-1:1996, definition 3.3.1.

3.2.4
authenticity
quality of being authentic or of established authority for truth and correctness

NOTE An authentic record is one that can be proven to be what it purports to be, to have been created or sent by persons purporting to have created or sent it and to have been created or sent at the time purported [Records Management, NHS Code of Practice].

3.2.5
authentication
process of reliably identifying security subjects by securely associating an identifier and its authenticator

NOTE See also **data origin authentication** (3.2.11).

3.2.6
authorization
granting of rights, which includes the granting of access based on access rights

ISO 7498-2:1989, definition 3.3.10.

3.2.7
availability
property of being accessible and usable upon demand by an authorized entity

ISO 7498-2:1989, definition 3.3.11.

3.2.8
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

ISO 7498-2:1989, definition 3.3.16.

3.2.9
cryptography
discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

ISO 7498-2:1989, definition 3.3.20.

3.2.10
data integrity
property that data have not been altered or destroyed in an unauthorized manner

ISO 7498-2:1989, definition 3.3.21.

3.2.11
data origin authentication
corroboration that the source of data received is as claimed

ISO 7498-2:1989, definition 3.3.22.

3.2.12
decryption
process of obtaining, from a cipher text, the original corresponding data

ISO/IEC 2382-8:1998, definition 08-03-04.

3.2.13
digital signature
data appended to, or a cryptographic transformation [see **cryptography** (3.2.9)] of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient

ISO 7498-2:1989, definition 3.3.26.

3.2.14
identity authentication
identity validation
performance of tests to enable a data processing system to recognise entities

ISO/IEC 2382-8:1998, definition 08.04.12.

3.2.15
identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

ENV 13608-1:2000.

3.2.16
integrity
proof that the message content has not altered, deliberately or accidentally in any way, during transmission

3.2.17
key
sequence of symbols that controls the operations of encipherment and decipherment

ISO 7498-2:1989, definition 3.3.32.

3.2.18
key management
generation, storage, distribution, deletion, archiving and application of keys in accordance with a **security policy** (3.2.22)

ISO 7498-2:1989, definition 3.3.33.

3.2.19
non-repudiation
service that provides proof of the integrity and origin of data (both in an unforgivable relationship) which can be verified by any party

NOTE In a wider meaning, non-repudiation means there is unforgivable evidence that a specific action has occurred.

3.2.20
role
set of behaviours that is associated with a task

3.2.21
security
combination of availability, confidentiality, integrity and accountability

ENV 13608-1:2000.