TECHNICAL **ISO/TS**

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order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn.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.