TECHNICAL REPORT

ISO/TR 21548

First edition
2010-02-01

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

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

Reference number
ISO/TR 21548:2010(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 exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

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/TR 21548 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Introduction

This Technical Report is an informative report that provides additional guidance for implementation of requirements set by ISO/TS 21547. This Technical Report provides a guideline and method to select (from the requirements defined by ISO/TS 21547) a platform or domain-specific set of requirements fulfilling regulatory and normative requirements. The platform can be local, regional, national or cross-border. This Technical Report is planned to be used together with ISO/TS 21547.

This Technical Report provides guidelines that are intended as a supplement to ISO/TS 21547. The summary of additional guidelines is shown in the Annex A. This Technical Report defines a practical method and describes practical tools which can be used both in the development and management of eArchives fulfilling security requirements set by ISO/TS 21547. Most of those tools are not healthcare specific, but the selection and the implementation of security services and tools should always meet general and healthcare domain-specific requirements set by national legislation, norms and ethical codes.

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

1 Scope

This Technical Report is an implementation guide for ISO/TS 21547. This Technical Report will provide a methodology that will facilitate the implementation of ISO/TS 21547 in all organizations that have the responsibility to securely archive electronic health records for the long term. This Technical Report gives an overview of processes and factors to consider in organizations wishing to fulfil requirements set by ISO/TS 21547.

2 Terms and definitions

For purposes of this document, the terms and definitions listed in ISO/TS 21547 apply.

3 Abbreviated terms

— CDA Clinical documentation architecture

— EHR Electronic health record

— GP General practitioner

— HIS Hospital information system

— HL7 Health level 7

— ISMS Information security management system

— PKI Public Key Infrastructure

— LAN Local area network

— PACS Picture Archiving and Communication System

— TTP Trusted Third Party

— XML Extensible Mark-up Language

— VPN Virtual Private Network

4 eArchive and eArchiving process

4.1 eArchive

In healthcare an archive is defined as being an organization that intends to preserve health records for access and use for an identified group of consumers for a regulated period of time. An electronic archive (eArchive) preserves information in digital format. An eArchive has the responsibility of making information available in a correct and independently understandable form over a long period of time. To make this possible, the eArchive stores not only the data but also meta-information (e.g. representation, description, content and context information of the data, links between components and required preservation information).

Typically, an eArchive receives and stores fixed content of data (e.g. EHRs or parts of them) with associated metadata and policies. An alternative is to use the weeding method – the EHR system moves selected EHRs to a secondary storage area of the EHR system and stores the needed meta-information (including security rules) in a separate repository.

A typical method of storing fixed content of data is to preserve documents with associated metadata such as HL7, CDA or XML documents.

Digital archiving has a strong dependence on software. New file formats, software and platforms succeed each other rapidly and digital material requires constant maintenance in order to retain accuracy.

An eArchive can be a centralized organization or it can be federated (ISO/TS 21547:—, 6.2). In healthcare, the narrative patient record and images are typically archived separately (for example X-ray pictures are preserved by dedicated PACS-systems or by a RIS, ECGs and other bio-signals by their own dedicated systems).

The eArchive can serve only one dedicated user (e.g. one hospital or GP) in such a way that only health records created by this organization are preserved. On the other hand, one technical eArchive can store health records on behalf of many EHR systems. The federated eArchive can store records having the same security and preservation policy or it can preserve records having different security policies. In the latter case, the eArchive can be seen technically as one archive, but from a security point of view it includes many logical EHR-archives.

In practice, an eArchive can be a separate archive (“a secondary storage”) or an EHR system can manage all archiving functions without a separate technical eArchive. In the latter case the EHR system should meet security requirements set by national legislation and principles and requirements defined in ISO/TS 21547.

4.2 eArchiving process

ISO/TS 21547 has already defined that eArchiving is a holistic and long-term process. During this process, health records are moved between the EHR systems and the eArchive (the eArchive itself can be an external repository or a place in the EHR system where fixed records are stored). Figure 1 shows one practical model, where information is extracted from the local EHR-system database and transferred (in the form of documents) to the eArchive. The eArchive can also disclose preserved documents, which can be either viewed by end users or restored to the local database.

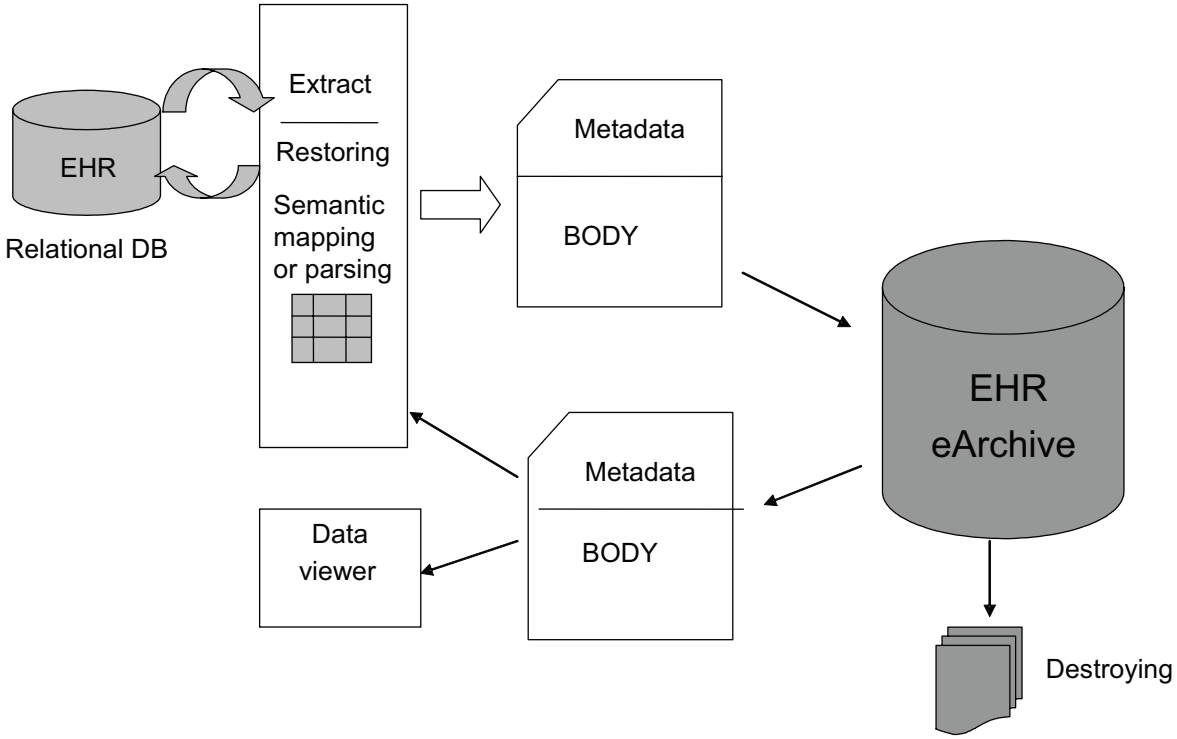

Figure 1 — Example of the eArchiving process

A typical eArchiving process consists of the following phases. The archiving process starts when information is extracted from the EHR-database. The next step is to make (if necessary) semantic mappings between local terminology and terminology used for the long term archiving (e.g. to maintain semantic interoperability). The third phase in this process is the generation of the archival packet (e.g. data and its metadata), which is sent to the eArchive. The eArchive stores received information in a fixed format for a defined period of time. The eArchive sends the requested information packets back to the EHR system, typically in the same format as that in which the information has been received. The eArchive can also destroy records. At the level of an EHR system the information can be either restored to the local database or viewed by the end user without restoration. If it is necessary to maintain semantic interoperability, the EHR system information will parse received information before it is restored.

Countries differ in their definition of the eArchiving process: it can cover the whole lifecycle of the EHR or only a part of it. In Finland (ISO/TS 21547:—, Annex A) the eArchiving process starts when patient information is initially created by the service provider and ends after the destruction of the record. In this case the service provider organization should manage the whole eArchiving process.

In the UK (ISO/TS 21547:— Annex B), archives are records appraised for permanent preservation and the term *archiving* is used to describe permanent preservation of records in the Place of Deposit.

Because the patient documents are dynamic during the care process, the information provider (typically a patient information system or Hospital Information System) transfers patient documents to the eArchive for long-term preservation at the time when the care process is ended and the patient's documents have been signed by the responsible clinician(s).

It is not always easy to define exactly the time when the care process is ended. In the case of hospital inpatient care this is typically the discharge time. Outpatient care, prevention and rehabilitation do not, in many cases, have a well-defined end point. Therefore, healthcare service organizations should define a minimum period after which the records of non-active patients should be extracted for long-term archiving. This period can also be defined by national legislation.

ISO/TS 21547 has defined the eArchiving process as including the following security services:

— security services when data are captured from the EHR system to the form defined and accepted by the eArchive;

— creation of security information (security metadata) connected to the record or data objects, and the linkage of this information to the data;

— security services needed to create the access request to the archive;

— security services needed during the data transfer from the EHR system to the eArchive and vice versa;

— security services needed by the eArchive to create a secure archival “packet” for long-term preservation;

— security services during the preservation period and in the event of data disclosure;

— security services needed to view and restore disclosed data;

— security services needed to prove the non-repudiation of the eArchiving process.

Data can be transferred from the EHR system to the eArchive using different technologies. One method is to send health records to the archive in the form of digital documents (for example in the form of XML or a HL7CDA document). Another possibility is to use the EN 13606 extract model or HL7 R3 messages to move information to the eArchive. It is outside the scope of this Technical Report to comment on specific technology in use.

The whole eArchiving process should be documented. This documentation should describe all participants and their roles and responsibilities (ISO 15489-1:2001, 9.10). Typical participants in the eArchiving process are: health service providers, telecommunication operators, the eArchive, and customers as patients and citizens.

4.3 Backup and recovery

The backup system is a method of copying electronic records to prevent loss through system failures (ISO/TR 15489-2). The backup includes multiple copies of records and dispersed storage locations for backup copies. Backups of health records are used to restore the archived information to its original state after any disaster (ISO/TS 21547:—, 6.2.1). Backup is also a part of the records management process of the archive. The backup system should guarantee the integrity, confidentiality and availability of EHRs.

A backup utility is typically a part of the operation system of the eArchive, but separate backup applications also exist.

The eArchive shall make regular backups (ISO/IEC 27799:2008, 7.6.5.1). To prevent data loss or erosion, the reliability of backups should be tested regularly. It is also necessary that information professionals managing the eArchive have been both educated and trained to make backups.

The eArchive should have a recovery plan to prove the availability of records after a disaster. The functionality of backups should be tested regularly.

5 Environment of the eArchive

ISO/TS Health Informatics — Security Requirements for Archiving of Electronic Health Records, has defined the typical environment of the eArchive. Because healthcare ICT is very dynamic, the number of information producers and customers will change. The environment of the eArchive should be fully controlled and the eArchive should maintain an online information database of all data producers and customers.

6 Responsibilities and policies

6.1 General

Responsibilities among data producers, the eArchive and customers should be clearly defined, fully documented and regularly maintained at all levels in the organization (ISO/TS 21547). This Technical Report provides additional guidance on those responsibilities.

All participants (e.g. EHR systems, the eArchive and organizations offering communication services) should define and document their own domain-specific security and data protection policies covering records management inside their domain. ISO/TS 21547:—, Clause 10, states that any system archiving electronic health records (e.g. eArchive) should have a well-defined and documented:

— archiving policy;

— security policy;

— privacy protection policy.

All domain-specific policies should be bridged together to form a comprehensive security and data protection policy for the whole eArchiving process.

Organizations should ensure that defined policies are implemented and maintained at all levels in the organization. Support of these policies by all employees is necessary at all times.

This Technical Report provides additional guidance on those policies.

6.2 Responsibilities

6.2.1 Introduction

From a security standpoint, the eArchiving process should be understood as a holistic system (ISO/TS 21547:—, 6.2). It is outside the scope of this Technical Report to define security responsibilities for the management of active EHRs used by the health organization in direct care or treatment.

The objective of defining responsibilities and inter-relationships is to maintain an eArchiving process for long-term preservation of EHRs that meets the security and data protection needs of internal and external stakeholders. In healthcare, security responsibilities can be derived from medical ethics, legislation, norms, standards, good practices and guidelines.

All participants in the eArchiving process have both domain-specific and common responsibilities. It is necessary to define responsibilities connected to the eArchiving process in such a way that no gaps exist. It should always be clear who is responsible for taking the necessary action (ISO 15489-1).

In healthcare, typically the service provider has the responsibility for archiving health records. It can do this by itself or it can procure the necessary archiving services from an external organization. Where the archiving of EHRs is outsourced to an external archiving organization, responsibilities for security management should be explicitly defined between contractors. It is important to ensure that they meet the standards laid down in the organization's policies (ISO 15489-1).

It is necessary to clearly define the security and privacy protection responsibilities between the EHR system and the eArchive. Responsibilities should be derived from existing legislation and norms. More practically, the eArchive and the health organization should have a written document or contract in which all responsibilities are defined.

eArchiving professionals and information managers have the primary responsibility for the implementation of Technical Specifications. In particular, they establish implemented procedures and processes. It is also their responsibility to implement other International Standards such as ISO 15489-1 and ISO 27799.

6.2.2 Responsibilities of the eArchive

The main tasks of the eArchive are to securely preserve health records for a regulated period of time and to make stored information available. The eArchive has the responsibility to make EHRs available for authorized users and for acceptable purposes. The eArchive also has the responsibility to ensure that records are not disclosed to unauthorized persons, processes or entities. Additionally, the eArchive has the responsibility to manage migrations in such a way that the integrity of the record is secured and that the process does not affect the characteristics of the record (ISO 15489-1). The eArchive may also have the responsibility to prove the non-repudiation of all these activities if national legislation so stipulates.

During the long preservation time, it is possible that regulations, access rules and storage time norms can change. The eArchive should regularly check for possible changes and, if necessary, update its internal rules, procedures and records management software. If necessary, the archive can also update the archival metadata of EHRs (for example change the preservation time information of the EHR). All changes should be documented.

The eArchive discloses stored records to other computer systems for further processing. The archive can disclose records in the form of messages or through online access services.

Security responsibilities of all stakeholders participating in the eArchiving process should be defined, including those of professionals managing the eArchive and its records. The latter requires that the eArchive define responsibilities of all its employees involved in records management (ISO/TR 15489-2). Responsibilities should be included in policy documents and formal contracts.

The eArchive should collect, store and make available all audit logs and prove both the integrity and non-repudiation of those logs.

6.2.3 Responsibilities of the EHR system

The “ownership” of EHRs is not closely or uniformly defined in most countries, but in the health care domain we can say that organizations controlling and managing EHRs have the stewardship of them. Typically a national law, decree or guideline defines:

— who has control responsibilities for the management of EHRs;

— when the archiving process is initiated, where and by whom;

— who is responsible for the management of the archiving process (e.g. the archiving department of the hospital or the chief medical doctor).

It is the responsibility of the EHR system to capture information that will be transferred for archiving from its local information systems (e.g. EHR system, laboratory system, radiological system or primary care information system) and add to the captured data, security information required for long-term eArchiving. Metadata needed for long-term preservation of EHRs should be added to the captured information. ISO 23081-1 as well as existing national standards and norms can be used in defining the actual content of the required meta-information.

It is also the responsibility of the EHR system to ensure that only those persons, processes and entities having the right to access archived records can use applications developed for this purpose. This can be realised using a role based access control service (RBAC).

The EHR system has the responsibility to generate and transfer all necessary information required for data disclosure to the archive. Depending on national legislation, this information can include:

— the certification of the existence of a patient-clinician relationship;

— patient consent information;

— information about the purpose of requested data;