DRAFT FOR DEVELOPMENT

DD ISO/TS 21547:2010

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

ICS 35.240.80

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

British Standards
Document Sharing Hub

Full document details: DD ISO/TS 21547:2010

# National foreword

This Draft for Development is the UK implementation of ISO/TS 21547:2010.

**This publication is not to be regarded as a British Standard.**

It is being issued in the Draft for Development series of publications and is of a provisional nature. It should be applied on this provisional basis, so that information and experience of its practical application can be obtained.

Comments arising from the use of this Draft for Development are requested so that UK experience can be reported to the international organization responsible for its conversion to an international standard. A review of this publication will be initiated not later than 3 years after its publication by the international organization so that a decision can be taken on its status. Notification of the start of the review period will be made in an announcement in the appropriate issue of Update Standards.

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into an international Standard, to extend the life of the Technical Specification or to withdraw it. Comments should be sent to the Secretary of the responsible BSI Technical Committee at British Standards House, 389 Chiswick High Road, London W4 4AL.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This Draft for Development was published under the authority of the Standards Policy and Strategy Committee on 31 March 2010.

© BSI 2010

ISBN 978 0 580 63721 6

**Amendments/corrigenda issued since publication**

| Date | Comments |
|---|---|
| | |
| | |
| | |
| | |

Documents
Document Sharing Hub

Full document details: DD ISO/TS 21547:2010

# 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)

Documents
Document Sharing Hub
© ISO 2010

Full document details: DD ISO/TS 21547:2010

**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2010

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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



© ISO 2010 – All rights reserved

Documents
Document Sharing Hub

Full document details: DD ISO/TS 21547:2010

# Contents

Page

**Foreword** ..... iv

**Introduction** ..... v

**1 Scope** ..... 1

**2 Normative references** ..... 2

**3 Terms and definitions** ..... 2
**3.1 General terms** ..... 2
**3.2 Security services terms** ..... 5

**4 Abbreviated terms** ..... 8

**5 General** ..... 9

**6 EHR-archive and eArchiving process** ..... 10
**6.1 EHR and record** ..... 10
**6.2 Archiving** ..... 12
**6.3 EHR-archive** ..... 13
**6.4 Backup versus EHR-archive** ..... 14
**6.5 Elements of the EHR-archive** ..... 14
**6.6 Types of EHR-archive** ..... 15
**6.7 Online storage** ..... 17
**6.8 The eArchiving process for EHRs** ..... 17
**6.9 eArchiving process and records management** ..... 19

**7 Environment of the EHR-archive** ..... 21

**8 Policies and responsibilities** ..... 22
**8.1 Responsibilities** ..... 22
**8.2 Policies** ..... 24

**9 Security and privacy protection architecture** ..... 25

**10 Security and privacy protection requirements for the eArchiving process** ..... 25
**10.1 Overview** ..... 25
**10.2 Policies and responsibilities** ..... 26
**10.3 Requirements derived from legislation** ..... 27
**10.4 Requirements for availability** ..... 30
**10.5 Requirements for integrity** ..... 34
**10.6 Requirements for confidentiality** ..... 36
**10.7 Requirement for non-repudiation** ..... 37

**Annex A** (informative) **Framework for long-term archiving of EHRs in Finland** ..... 39

**Annex B** (informative) **Framework for digital archiving of health records in the UK** ..... 45

**Annex C** (informative) **Framework for digital archiving of health records in Japan** ..... 53

**Annex D** (informative) **Framework for digital archiving of health records in the USA — Rules and requirements derived from HIPAA** ..... 56

**Annex E** (informative) **Comparison of ISO 15489-1 and ISO/TS 21547 security requirements for archiving of electronic health records** ..... 59

**Annex F** (normative) **Summary of normative requirements** ..... 71

**Bibliography** ..... 76

© ISO 2010 – All rights reserved


Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

## 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*.


© ISO 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

# 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;

© ISO 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

— 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.


© ISO 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

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.

Documents
Document Sharing Hub

© ISO 2010 – All rights reserved


Full document details: DD ISO/TS 21547:2010

Documents
Document Sharing Hub

Full document details: DD ISO/TS 21547:2010

# 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.

© ISO 2010 – All rights reserved



Documents
Document Sharing Hub

Full document details: DD ISO/TS 21547:2010

— 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.


© ISO 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

**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.

© ISO 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

**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


© ISO 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

**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.

© ISO 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

**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.


© ISO 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

**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.

© ISO 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

**3.2.22**
**security policy**
plan or course of action adopted for providing computer security

ISO/IEC 2382-8:1998, definition 08.01.06.

EXAMPLE A set of laws, rules and practices that regulate how sensitive information is managed and distributed within a specific system.

**3.2.23**
**security service**
service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers

ISO 7498-2:1989, definition 3.3.51.

**3.2.24**
**information security**
protection of information from (accidental or intentional) unauthorized access, use, disclosure, disruption, modification or destruction

**3.2.25**
**information security policy**
document that states, in writing, how an organization plans to protect its physical and information technology assets

**3.2.26**
**security classification**
category to which personal information and material is assigned to denote the degree of damage that unauthorized disclosure would cause a person or his/her relations and to denote the degree of protection required

## 4 Abbreviated terms

— CDA Clinical documentation architecture

— EHR Electronic health record

— HL7 Health level 7

— ISMS Information security management system

— PKI Public key infrastructure

— LAN Local area network

— NHS National Health Service

— PACS Picture archiving and communication system

— TTP Trusted third party

— XML Extensible mark-up language

— VPN Virtual private network


© ISO 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

## 5 General

Healthcare service providers are realizing many benefits when they are using digital technology for archiving health records. The most commonly mentioned benefits are:

— cost savings;

— new possibilities for information sharing;

— new ways to support clinical workflows;

— data are available online on a 24 h/7 d basis.

From an archiving viewpoint, we have to understand that archiving personal health information in digital format produces not only benefits, it also gives rise to new security and confidentiality problems:

— digital material requires constant maintenance in order to stay alive;

— digital information can be easily corrupted, disseminated and copied without recognition;

— digitally stored information is easily accessed over traditional organizational borderlines;

— digital documents have a shorter lifecycle than paper documents;

— digital documents are usually closely linked to media, and any media we currently know may soon become inaccessible;

— information retrieval is dependent on software versions used;

— risks due to malicious code and viruses.

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

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

— healthcare data objects/documents are dynamic during the whole lifetime;

— healthcare data are context sensitive;

— the data content is sensitive;

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

— there is a strong legal framework regulating who can access what and when;

— data objects have context, purpose and sensitivity based access/disclose rules;

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

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

© ISO 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

# 6 EHR-archive and eArchiving process

## 6.1 EHR and record

### 6.1.1 Overview

In this Technical Specification we are defining security requirements for the long-term preservation of EHRs. ISO 15489-1 is another International Standard already used in healthcare. Therefore it is necessary to understand special features of the EHR.

There are a great variety of definitions for a record. A record is:

— anything (e.g. document) providing permanent evidence of or information about past events;

— a permanent form;

— a document that can serve as legal evidence of a transaction;

— recorded information;

— a collection of related data;

— what you retrieve when you search in a database;

— a written document;

— an individual component of a database;

— a collection of related fields;

— a database record consisting of one set of tuples for a given relational table; in a relational database, records correspond to rows in each table;

— a composite variable that can store data values of different types.

ISO 15489-1 has defined the record in the following way:

*A record is information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.*

The definition of health record varies in different countries. A number of definitions for the term “EHR" also exist worldwide. There is no internationally accepted definition for the EHR (see ISO/TS 18308). Differences reflect different shades of meaning between different countries and organizations. It is possible that the information content of the EHR is restricted compared to the content of the Health Record. Generally we can say that the Health Record may not equal EHR.

Two widely used definitions for the EHR are:

a) a comprehensive, structured set of clinical, demographic, environmental, social, and financial data and information in electronic form documenting the healthcare given to a single individual (ASTM E1769);

b) a longitudinal collection (e.g. produced by encounters in one or more care settings) of personal health information for a single individual, entered or accepted by a healthcare provider, and stored electronically (HINA 2000).

It is also possible to speak about Regulated or Legal Health Records and Primary Records. AHIMA (American Health Information Management Association) defines the legal health record as “generated at or for a healthcare organization as its business records and is the record that would be released upon request”.


© ISO 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

To highlight how the EHR has been defined in different countries, we can take two examples, the UK and Finland. In the UK, the NHS the Code of Practice speaks about NHS records. Typical NHS records are:

— patient records (e.g. GP medical record and speciality records);

— records of private patients;

— some registers (e.g. accident and operating theatre registers);

— administrative records (e.g. financial and accounting records and notes).

In Finland the EHR is a legal record of a single patient created by the service provider organization producing the care or treatment. This EHR is cumulative and lifelong at the level of a service provider. In Finland the Act on Patients' Rights defines service provider organizations (e.g. secondary care hospital, primary healthcare centre, occupational care service provider and a single private physician). This means that in Finland a citizen can have many separate EHRs (which are cumulative at service provider organization level).

We can also speak about logical EHRs. A typical logical EHR is:

— an institutional EHR;

— a longitudinal EHR;

— a lifelong EHR.

The institutional EHR can be:

— a single physical record including all information on one inpatient or outpatient visit or treatment;

— a combination of records created by a service provider organization (e.g. lab or X-ray records and records created by specialities) during a patient's visit or an episode of care; in this case separate records are typically linked together to form a logical EHR;

— a cumulative personal record including information on all visits to one service provider organization; the record can be a single physical cumulative record or it can include many linked cumulative sub-records (or folders);

— a collection of selected cross-organizational patient records.

Independent of the way the EHR is archived (e.g. as a single record or in the form of connected separate records), it is necessary to prove not only the integrity of one record but also the integrity of all connected records forming the logical EHR during the whole preservation time.

Typical solutions to manage an EHR including more that one fixed part are registration service, master index table and metadata technology.

A variety of computer-based technologies to store and manage EHRs exist. Typical technologies used are:

— relational databases;

— document management systems;

— image management systems;

— picture management systems;

— specialized systems storing biosignals.

© ISO 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

Documents can also come in many formats, for example HL7 CDA, PDF or Word. Images can come in a variety of formats such as JPG and TIFF.

One dimension of the EHR is the location where it is technically stored and managed. Typically it is stored in the computer system of one service provider.

### 6.1.2 Distributed EHR architecture

Some countries use the distributed record architecture model. In this architecture the EHR can be defined as a composite of physically distributed records (e.g. a summary of linked cross-organizational EHRs). In a distributed model, it is possible that the management of the EHR is not in the hands of a single service provider. Therefore, the management of integrity of distributed EHRs requires specific actions.

Technically, EHRs can be linked together either horizontally or vertically. In the case of a vertically linked, distributed EHR, the link point is typically a master index file. It is also possible to duplicate some content of distributed parts in the master repository (the SPINE in the UK is just this kind of master index repository).

### 6.1.3 Healthcare-specific features of the EHR

There are many healthcare-specific features in the EHR. One of them is that during its lifetime the content of the EHR includes both dynamic and fixed parts. The content is dynamic during the direct care or treatment process. Many health professionals and other persons who participate in the care process can manage the content of the EHR based on their roles and privileges. It is also typical that some entities (e.g. automatic analyser) can automatically add new information to the EHR.

In most countries the content of the health record or some parts of it[2)] must be signed, after the care episode or treatment, by the responsible physician in such a way that it is not possible to make modifications to the record. After signature the content of the record shall not be changed i.e. the record can be called a fixed record. Depending on the EHR-architecture, it can include only one signed part or there can be a combination of many separately signed parts.

The cumulative EHR can include many (previously signed) fixed parts and one dynamic part, the contents of which can be updated during the ongoing care or treatment process.

When thinking about eArchiving or long-term preservation, the EHR should be understood as a logical record. It can be a single physical record, any combination of connected/linked (sub)records and a composite of EHRs.

Fixed records forming the logical EHR are preserved either in the EHR-archive or inside the EHR-system. This means that the eArchive can be a separate local or outsourced archive, or the eArchiving is just one function of the EHR-system used by the service provider organization.

The starting point of this Technical Specification is the long-term preservation of a logical EHR, irrespective of how many fixed parts it includes. Physically the EHR-archive can be centralized or distributed (for example the administrative part can be nationally centralized, while other parts are archived at the local or regional level).

## 6.2 Archiving

Archiving is much more than just a simple preservation of papers, microfilms or bits. Archiving is a combination of:

— data reception management;

— data preservation and accessing management;

— security and privacy protection management;

---

2) Typically, the primary (legal) EHR will be signed by the physician responsible. It is possible that some components of the EHR, such as laboratory tests, will not be signed by a physician.


© ISO 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

— records management;

— information description methods;

— storage media technology.

## 6.3 EHR-archive

In healthcare an archive is defined as an organization that intends to preserve EHRs for access and use for an identified group of consumers for a regulated period of time. The archive preserves and discloses EHRs or makes them accessible for an identified group of users. Traditionally in healthcare the archive has been the storage of paper documents and pictures. In many cases, even when the service provider is using an EHR-system, it has been a common practice to print the content of digital records on paper or in a film format for long-term preservation purposes.

An electronic archive preserves information in digital format. Differences between paper and digital preservation are extreme. Digital archiving is strongly dependent on software. New file formats, software, and platforms succeed each other rapidly and digital material requires constant maintenance in order to stay alive. In the case of digital archiving there is a danger that not only the functionality but also the structure of the EHR, and the context of archived bits and data streams can be lost after hardware and software migrations.

An electronic archive is designed to make information available in a correct and independently understandable form over a long time. In order for the preserved information to be both accessible and understandable for the customers needing it, even after a long time, information other than the actual data will also have to be stored. We need to know what the data object is and what it is meant to do. The data should also be undamaged, complete and authentic: it is what we believe it to be. This leads to a situation where the EHR-archive 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).

The EHR-archive stores a fixed content of data (patients' health-related data) with associated metadata and policies. The fixed content of data is (can be) defined automatically by an application before it is sent to archive. After the EHR is archived, its content cannot be modified or deleted by the archive before its preservation time expires. The EHR-archive distributes fixed records; it cannot make any partial delivery of the signed EHR.

In some countries, the content of the EHR can have a dynamic nature during its lifetime. The patient record can also be lifelong and cumulative (see Annex A). The dynamic nature means that the archived fixed record can be sent back to the service provider for the next patient visit. During the care episode new information will be added to the original record before the updated record is sent back to the archive. Even in this case the archive preserves fixed records, but during its lifetime the content of the EHR can be cumulative.

In healthcare, it is typically not allowed (based on regulations) to make any changes to the content of the record after it has been signed by the physician responsible. This means that only new fixed data objects (components) can be added to the record stored before it is sent to the EHR-archive. Generally we can say that the EHR-archive in the healthcare environment has an “on-demand” nature and the content of a preserved EHR can grow.

There is also a digital preservation service called an “active EHR-archive”. This kind of EHR-archive supports random access to and updates of stored data. In practise the difference between an active EHR-archive and online repository is marginal.

A permanent archive in healthcare is a special type of archive that stores EHRs permanently.

NOTE 1 NHS Code of Practice (see Annex B) defines archives as records that are appraised as having permanent value. Some records will be selected as archives and sent to a repository that has been approved for the permanent preservation of records. This kind of repository can be classified as a permanent archive.

NOTE 2 In Finland small numbers of records are selected for permanent preservation. Those records are moved to the “end-archive” for research purposes.

In real life, the EHR-archive cannot stand alone. Interoperability with EHR-systems is required. Figure 1 shows how the EHR-system, a long-term EHR-archive and the permanent archive are connected.

Documents
Document Sharing Hub

© ISO 2010 – All rights reserved


Full document details: DD ISO/TS 21547:2010

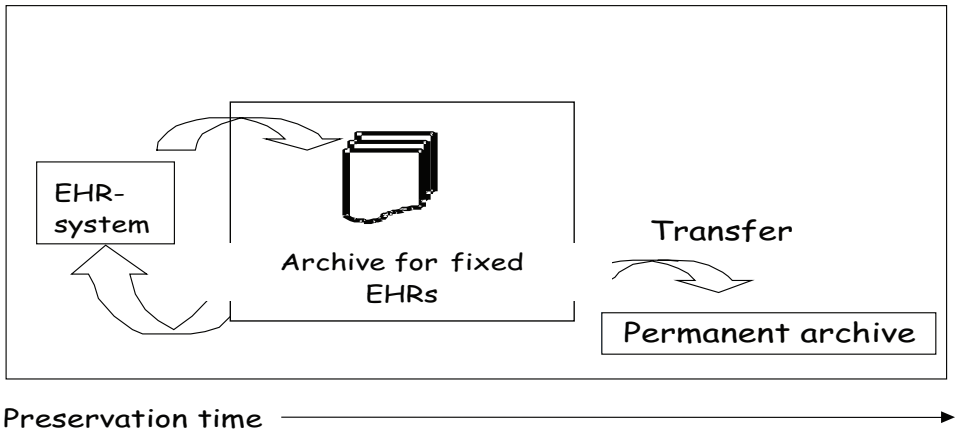


**Figure 1 — EHR-system, long-term EHR-archive and permanent archive**

## 6.4 Backup versus EHR-archive

The backup is a digital migration of information within the archive or an EHR-system. The backup is used to restore the data to their original state after any disaster. Typical backup methods are refreshment, mirroring, replication and transformation.

In the case of the long-term preservation of EHRs, backup cannot replace the EHR-archive, but the backup is one of the necessary functions of the archive.

## 6.5 Elements of the EHR-archive

ISO 14721 has defined the following four basic elements for the archive (see Figure 2):

— archival storage;

— preservation planning;

— data management (including request and access management);

— administration.


© ISO 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

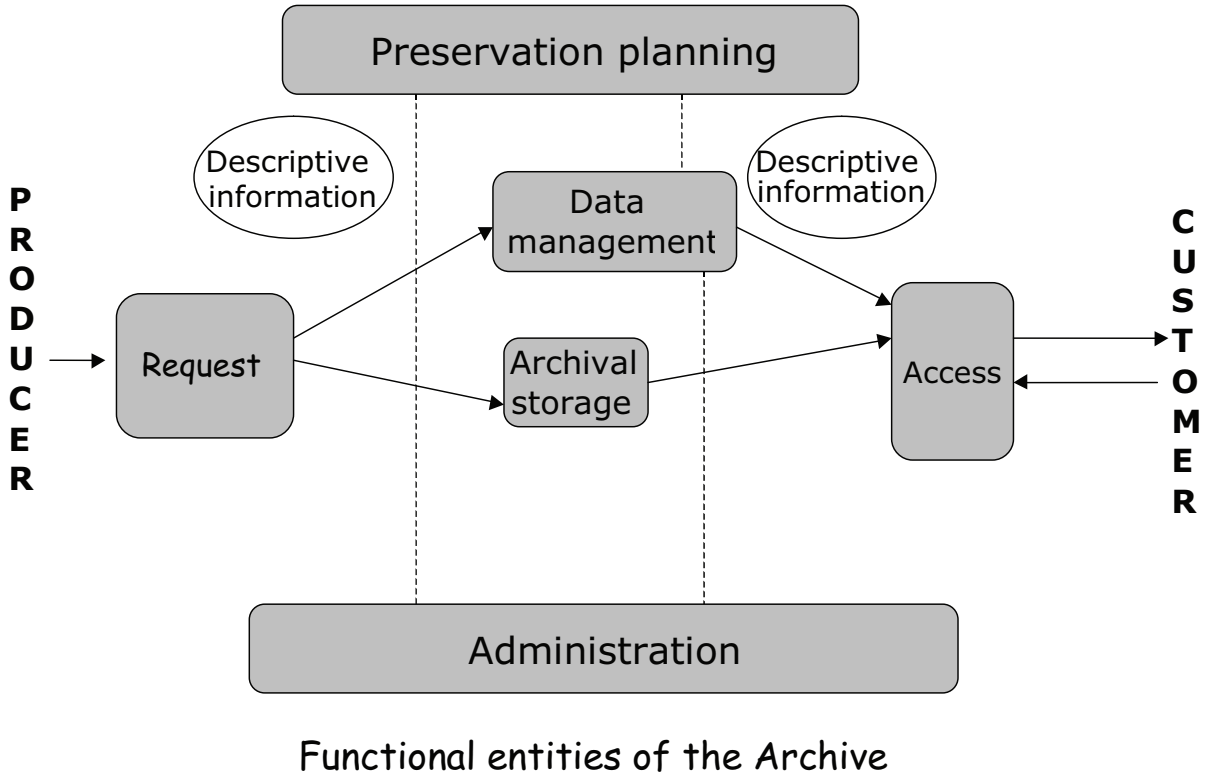


**Figure 2 — Elements of the open archive (ISO 14721)**

Those elements are also basic elements for any EHR-Archive.

## 6.6 Types of EHR-archive

The purpose of an EHR-system is to support the direct care process. During this process, the patient information is used and updated by a group of health professionals randomly and the integrity of data is not secured online. Put another way, the main purpose of the EHR-archive is just the long-term preservation of fixed patient records.

Different types of archive exist. An independent archive is a closed system aimed only at designated users. Co-operated archives have common standardized submission and dissemination methods but no common finding aids (e.g. no link repositories). Federated archives are based on the fact that different organizations have interest in the holdings of several archives. As the motive is to share some expensive resources, federated archives are systems with shared functional areas (ISO 14721).

An EHR-archive can, in actuality, be a separate archive (e.g. “secondary storage”) or an EHR-system can manage all archiving functions without a separate (technical) archive. Independent of which combination is used, the purposes of the EHR-archive and EHR-system are different.

Federation between an EHR-system and an archive typically exists within an organization, but regional solutions also exist. In this case, both the archive and the EHR-system share common privilege management and access control systems and they can also have common data searching services.

© ISO 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

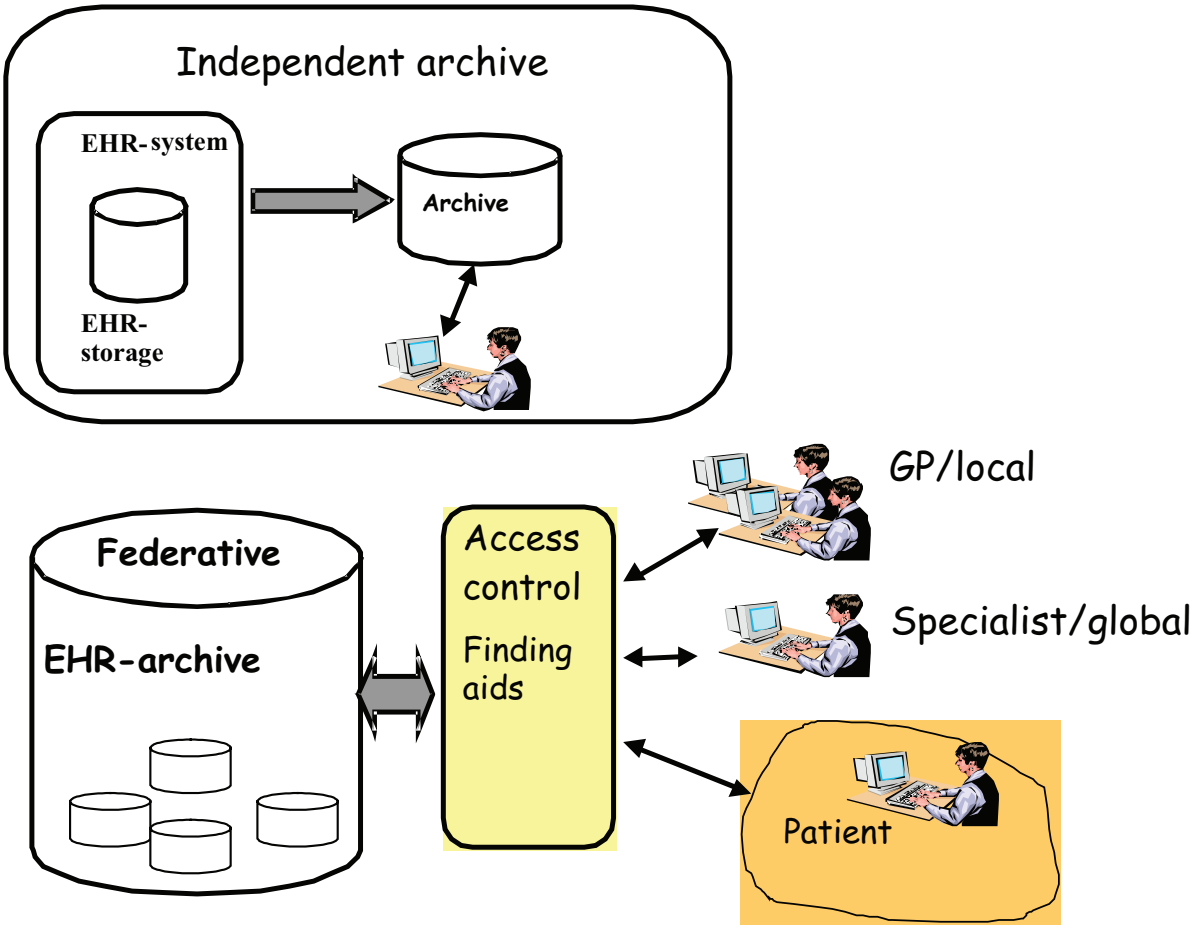


**Figure 3 — Independent and federated archives**

Federated archives provide access via common search aids (e.g. via a common catalogue or query distribution method). Archives having a common privilege management (a single access site) are examples of federated archives, see Figure 3.

A federated EHR-archive can also be created by linking geographically distributed EHRs together using a centralized master index repository. This repository can be regional and even national. One example of this kind of federated archiving system is the UK SPINE system. In SPINE, EHRs are preserved at local level, but selected parts of each patient record are copied to a common national repository (e.g. SPINE). The SPINE also includes common search aids to enable the access of local EHRs. In this case a patient can have many distributed records, but with the help of the SPINE services, it is possible to create a virtual personal EHR for all patients. One benefit of federated EHR-archives is the increased availability of patients' health information. However, a downside is maintaining the integrity of information located in SPINE and is, at the local level, a demanding task.

There are different ways to combine EHR-systems and the EHR-archive. An EHR-archive can be understood to be such an embedded part of the EHR-system that no formal archive exists at all. This kind of EHR-system has one centralized security policy, access control and privilege management services. Online electronic storage systems are typical of this kind of information system. Many patient information systems based on the utilization of relational databases seem to be this kind of system. It is necessary to remember that an archiving policy is still needed, and in this case the EHR-system also has to securely manage the long-term preservation of patient records.

The EHR-archive and EHR-systems can form a co-operative information system. In this case the archive communicates with the EHR-system, typically in the form of queries and answers. EHR-systems send and receive information from the archive. Typical of this kind of system is PACS (Picture Archiving System).


© ISO 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010

## 6.7 Online storage

Record systems called “online storage” exist in the healthcare environment. A typical application for online storage is digital image processing and preservation (e.g. a PACS system). Records maintained in those systems are aimed both at immediate work-flow support and long-term preservation of digitalized records. In many cases records are stored in the data repository using a vendor-specific format, but for interoperability purposes common data representation standards (e.g. DICOM) are used.

In many cases present online systems do not have a separate archive at all, but they are still undertaking the long-term preservation of EHRs. Even in this case, the preservation process must be legal and fulfil national security and privacy protection requirements set for long-term preservation. It is outside the scope of this Technical Specification to define security requirements for online EHR-systems, but selected requirements set by this Technical Specification can be used to implement necessary security and privacy protection services for online storage systems doing long-term preservation tasks.

## 6.8 The eArchiving process for EHRs

The eArchiving process in healthcare is both holistic and long-term. During this process, patient information is moved between the EHR-systems, the EHR-archive and customers. Throughout the time-span of preservation new fixed information packages can be repeatedly added to the EHR.

Typically the eArchiving process starts when information is extracted from the EHR-database. The EHR-system generates the archival packet (e.g. data and metadata), which is sent to the EHR-archive. The EHR-archive stores received information in fixed format for a defined period of time. The EHR-archive sends requested information packets back to the EHR-system; typically in the same format it has been received. The EHR-archive can also destroy EHRs.

There are differences between countries in how the eArchiving process is defined. In some cases the eArchiving process starts when the EHR is originally created by the EHR-system (legacy system) during the care process and ends when the regulated preservation time is reached, and the record is disposed of by the archive. On the other hand there are countries where the eArchiving process starts by the selection of records for permanent preservation and EHRs are stored by a specific archiving organization.

In Finland (see Annex A), the eArchiving process starts when patient information is originally created by the local service provider and ends after the destruction of the record. This means that the service provider organization must manage at the same time both active records inside its EHR-system and the external eArchiving process for fixed EHRs.

In the UK (see Annex B), archives are records appraised for permanent preservation and the term archiving is used in connection with the permanent preservation of records in the place of deposit. The NHS definition for record management covers the creation, storage, management and disposal of records. The NHS code of good practice is based on national requirements. In the UK, ISO 15489-1 is used as a record management standard.

The Japanese model for eArchiving of health records is based on the use of ISO 14721 and ISO 15489-1 (see Annex C). The eArchiving process only covers occurrences inside the EHR-archive.

Both the healthcare service provider and the archival authority of the EHR-archive have responsibilities during the eArchiving process. Responsibilities are typically defined by the national legislation. In some countries the service provider has the responsibility to securely manage the record during the whole archiving process (e.g. the EHR-archive is preserving EHRs “on behalf of the service provider”).

In the healthcare environment, the EHR-archive and EHR-systems are functioning together. There are different ways to realize this co-operation. Figure 4 describes a typical model, where the EHR-system and the EHR-archive communicate with each other using standardized messages. In this model the task of the EHR is to capture selected information from a local database (for example from a relational DB repository) and add necessary meta-information to the information packet (including data objects and metafile) before it is sent to the archive for long-term preservation. The archive receives information packets, adds meta-information required for archiving purposes to the data object, and finally stores those “archival packets”. The archive

© ISO 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: DD ISO/TS 21547:2010