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to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn.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

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

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.

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”.

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.

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.

— 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.

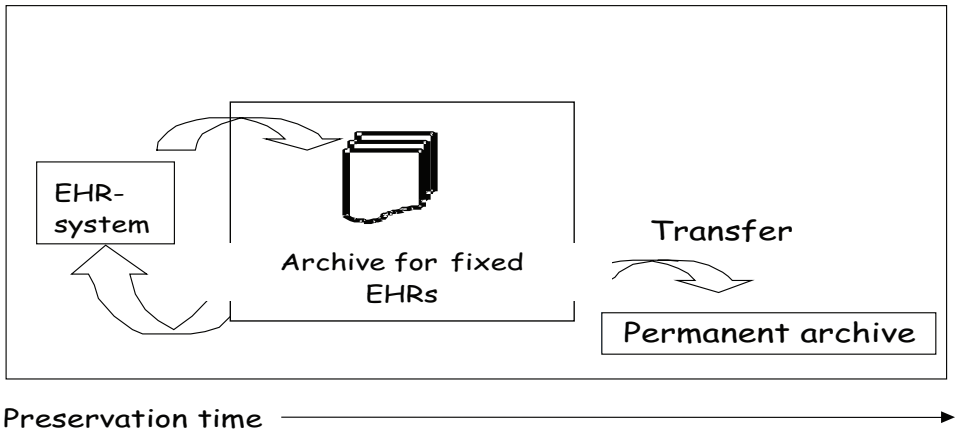

Figure 1 — EHR-system, long-term EHR-archive and permanent archive

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.

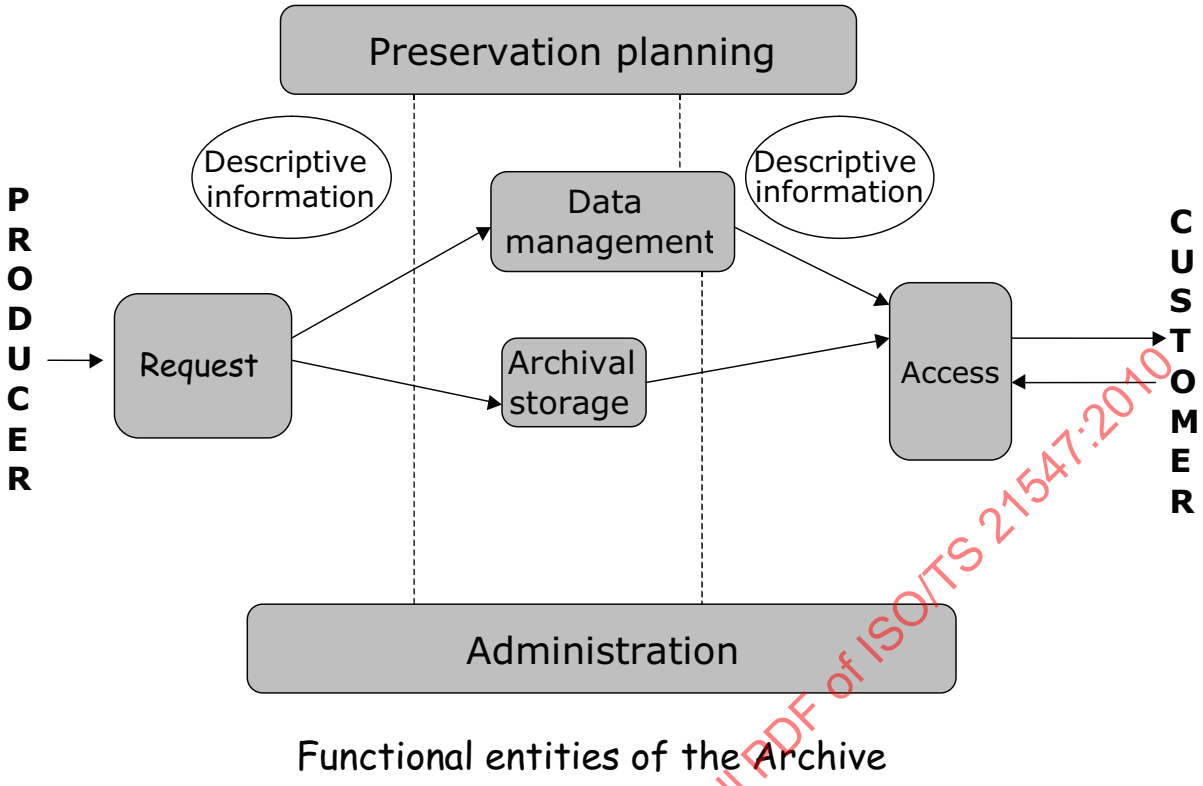

Figure 2 — Elements of the open archive (ISO 14721)

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.

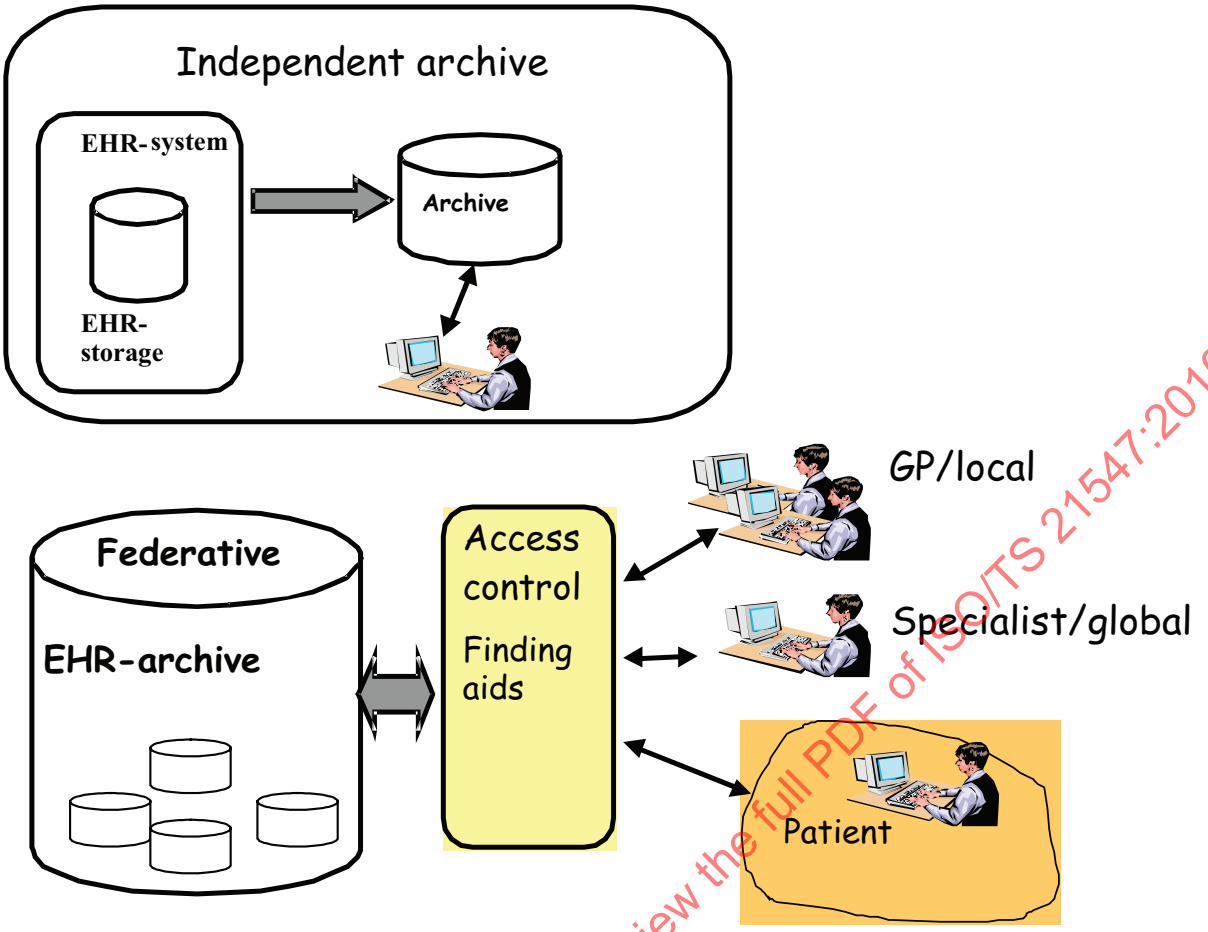

Figure 3 — Independent and federated archives

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).

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

discloses data objects based on requests from designated users. This cyclic archiving process described in Figure 4 covers the whole lifecycle of the EHR. The meta-information added to data before it is sent for long-term preservation also includes security and privacy protection information connected to all data objects.

Another model is to move inactive data from the online EHR-system to a secondary storage system. The security information of the EHR can be stored either in the metafile of the EHR or in a separate obligation repository. The stored data and meta-information are linked together (for example using unique identification). The secondary storage can be part of an online computer system or information can be stored using CD/DVD technology.

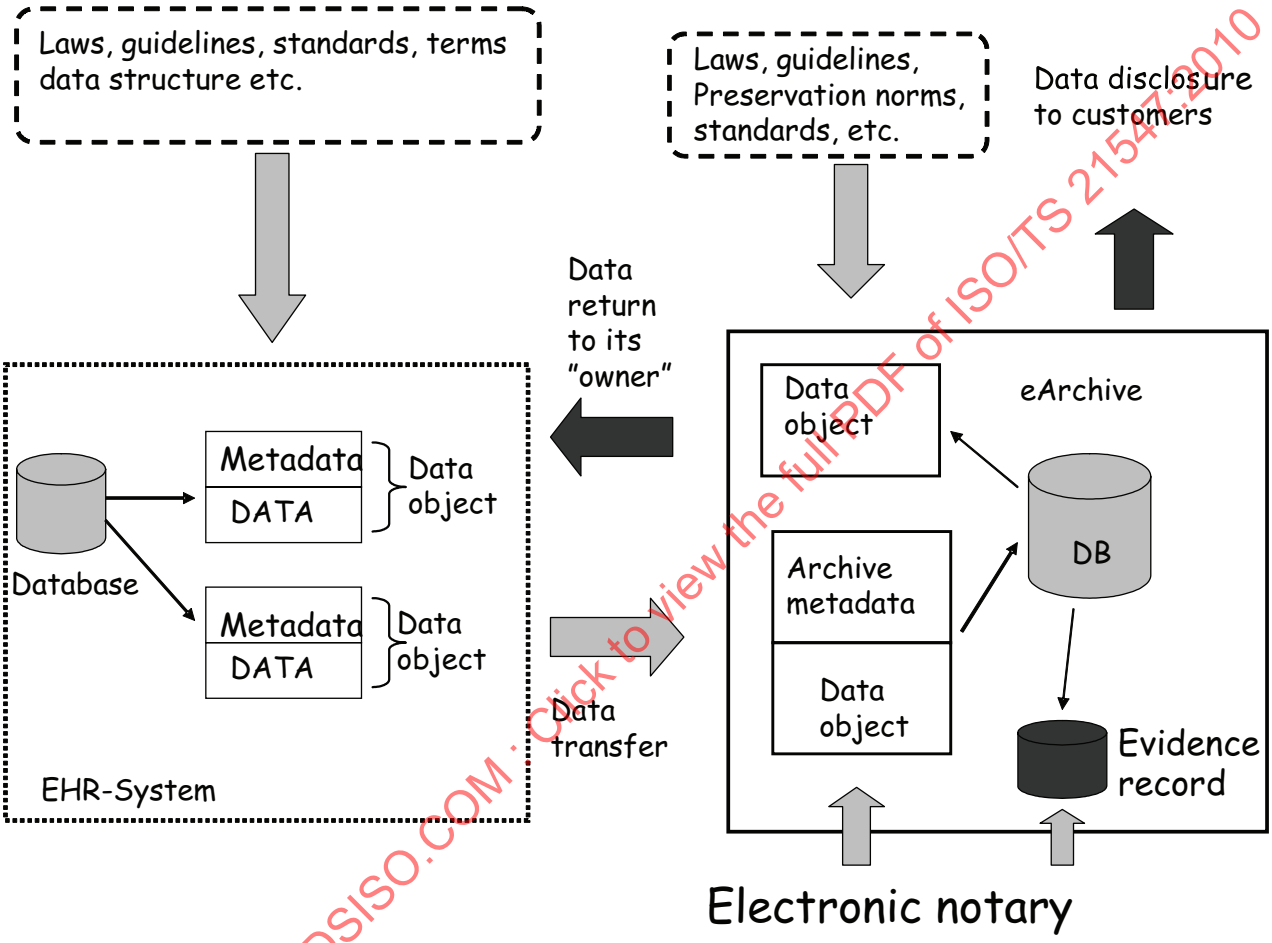

Figure 4 — A model of the eArchiving process

In this Technical Specification the eArchiving process includes the following activities:

— security services when data are captured from EHR-systems to the structure needed by the EHR-archive;

— creation of security information connected to data objects and the linking of this information to the data;

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

— services needed by the EHR-archive to create a secure data “packet” for long-term preservation;

— security services during the preservation time and in the case of data disclosure.

Data can be transferred from the EHR system files to the EHR-archive in different ways and using different technology. One practical method is to send health records to the archive as digital documents together with associated meta-information (for example in the header of an HL7 DCA document or the metadata can be stored in attributes of the data objects).

The EHR-archive can store the received documents in the form of fixed documents together with the connected meta-information. An alternative is to use the weeding method and move selected records to a secondary storage area of the EHR-systems and store the needed meta-information (including security rules) in a separate repository.

It is outside the scope of this Technical Specification to comment on the communication technology used between the EHR-system and the EHR-archive. The purpose of this Technical Specification is to describe technology-independent security requirements for the archiving process. It is also outside the scope of this Technical Specification to comment on the methods used for actual records management inside the EHR-archive and EHR-system. ISO 15489-1 can be used for those purposes.

6.9 eArchiving process and records management

ISO has developed two major documents for records management, ISO 15489-1 and ISO/TR 15489-2. The two-part ISO 15489 provides guidance for managing all types of records. The above-mentioned documents do not include the management of archiving of records within archival institutions.

The archiving of health records is more than just records management, but there are also similarities. The EHR is created and typically maintained inside the EHR-system. Records are captured and sent to the EHR-archive for long-term preservation by the EHR-system. Archived EHRs are managed during the preservation period by the EHR-archive.

The viewpoint of this Technical Specification is not limited to records management inside the EHR-system or the EHR-archive. Instead, it covers the whole long-term eArchiving process (see Figure 5) and it also gives healthcare-specific security requirements. This Technical Specification uses ISO 15489 and ISO 23081-1 and gives additional healthcare-specific security requirements. Figure 5 shows how this Technical Specification and ISO 15489 can be used together.

This Technical Specification gives additional requirements and guidelines for the management of a secure eArchiving process.

Both the EHR-system and the EHR-archive must, as a part of their internal management process, also manage health records (see Annex B and Annex C). Annex E compares security requirements set by ISO 15489 and this Technical Specification.

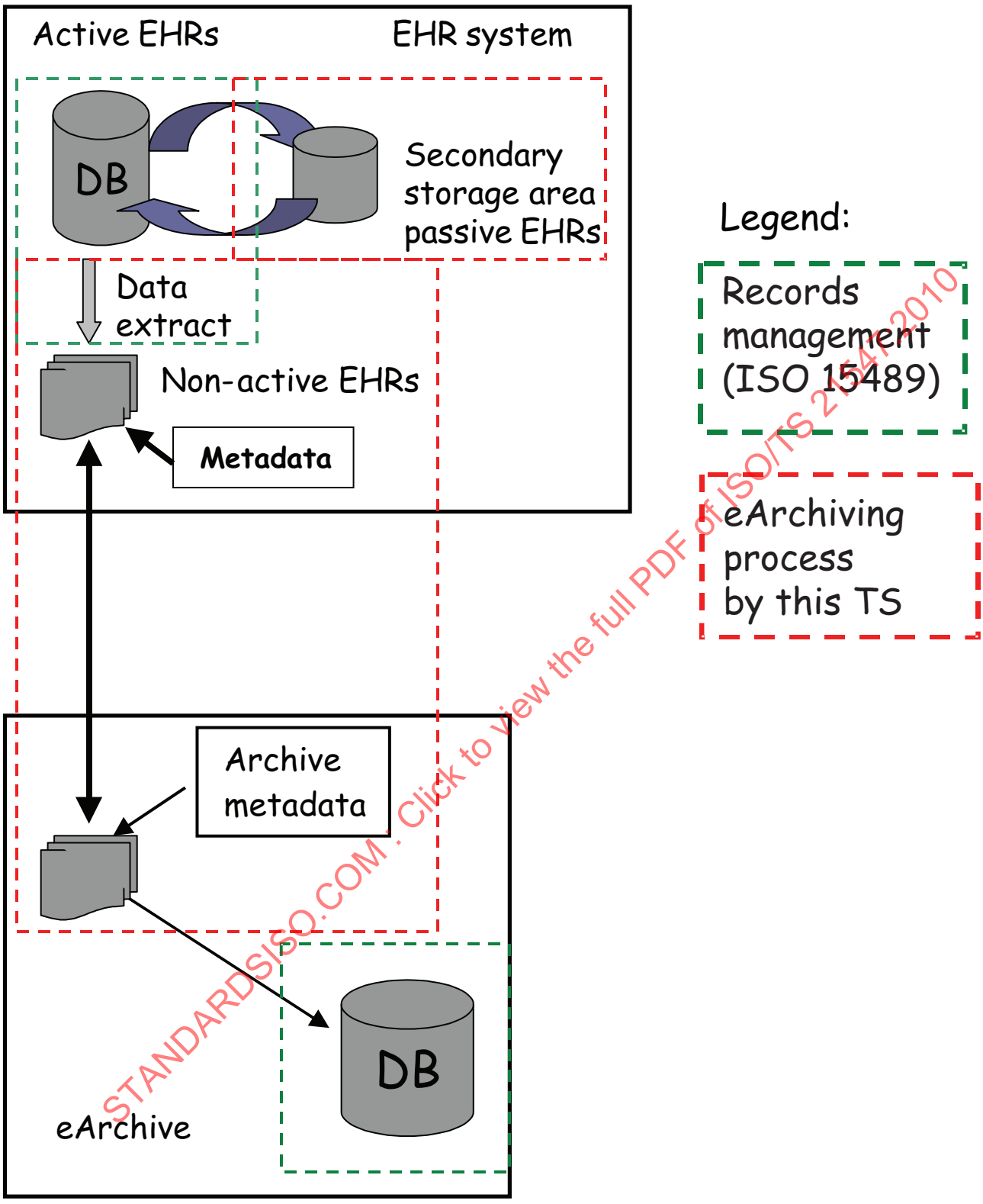

Figure 5 — Areas covered by the eArchiving process

7 Environment of the EHR-archive

Figure 6 shows the ISO 14721 model of an archiving environment. In the healthcare environment an information producer can be a:

— local EHR-system;

— foreign EHR-system;

— external laboratory, X-ray laboratory;

— health professional;

— patient/citizen;

— automatic instrument or analyser used by the patient at home;

— implanted measuring instrument.

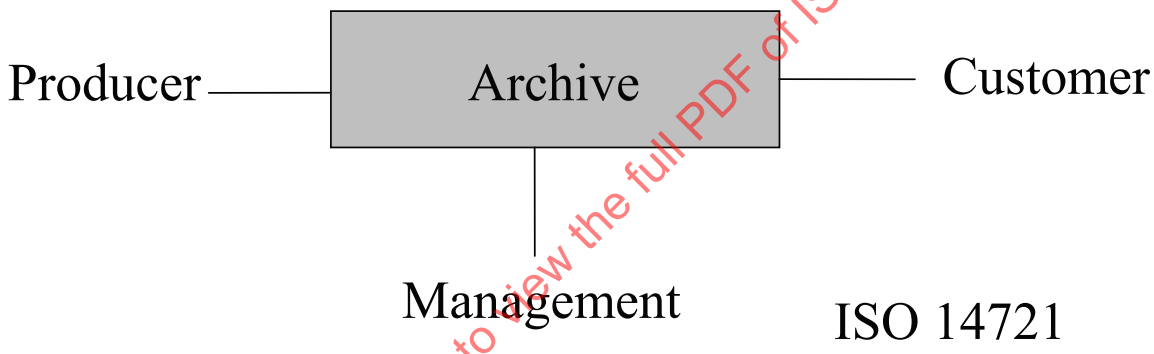

Figure 6 — The environment of the EHR-archive

Customers of an EHR-archive are persons or information systems that interact with the archive to find and access preserved information. In the healthcare environment typical customers of an archive are:

— healthcare organizations;

— EHR-systems;

— health professionals;

— civil servants (having the legal right to access preserved information);

— external laboratories;

— researchers;

— patients/consumers;

— citizens.

8 Policies and responsibilities

8.1 Responsibilities

8.1.1 Responsibilities of the EHR-archive

Electronic archiving of health records is a holistic process between data producers, customers and the EHR-archive. This process also includes responsibilities of all partners participating in the eArchiving process.

Basic responsibilities for an EHR-archive are:

— it negotiates for, and accepts appropriate information from, information producers;

— it obtains sufficient control of the information provided to support long-term preservation;

— it determines the users that make up its designated community and who should be able to understand the content provided;

— it follows documented policies and procedures that ensure the information is preserved against all reasonable contingencies and enables the information to be disseminated as authenticated copies of the originals or as traceable to the originals;

— it has the responsibility of maintaining the technical usability of stored EHRs;

— it makes the preserved information available;

— it continually reviews its policies and procedures.

In the healthcare environment it is necessary that citizens, patients, content creators and current and potential customers be able to trust the EHR-archive. From this point of view the EHR-archive will be a trusted repository, whose mission is to provide reliable, long-term access to managed digital resources to its designated community, now and in the future. To realize this, it is necessary to create policies, practices, and performance for the EHR-archive that can be audited and measured. It is also necessary to establish methodologies for system evaluation that meet community expectations of trustworthiness, make risk identification and have a risk management system.

Operational responsibilities of the EHR-archive can be divided into the four layers shown in Figure 7.

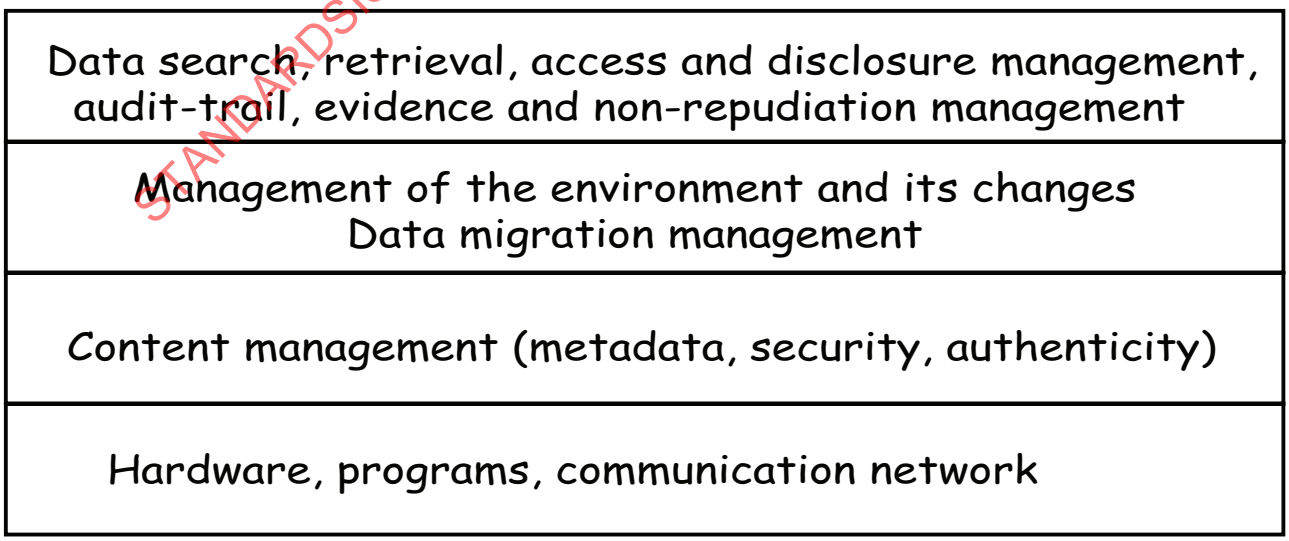

Figure 7 — Layers of operational responsibilities for the EHR-archive

More precise operational responsibilities are:

— receiving and handling the request for data preservation;

— preparing received data for preservation (e.g. creating the archival metadata);

— maintaining records management tasks inside the archive;

— data preservation and preservation management (this includes both the data and associated metadata);

— ensuring the availability of information;

— receiving and managing received access requests from customers;

— data disclosure;

— administrative functions;

— data destruction;

— auditing and monitoring the use and disclosure of data;

— managing the evidence of events.

Since the preservation times of patient records are long, it is probable that during the preservation period the archive will undergo several changes in the technology of preserving digital documents as well as conversions between storage media (see Figure 8). Therefore, the EHR-archive needs a migration plan in order to guarantee that the information does not change.

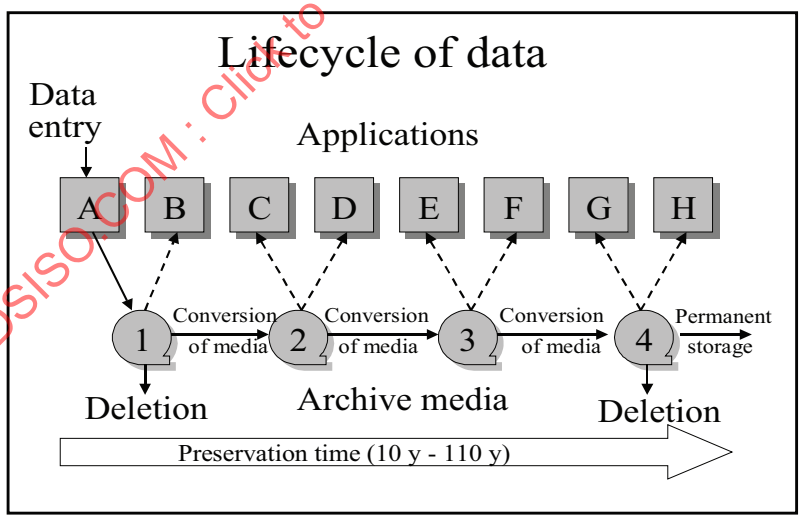

Figure 8 — Preservation time of the EHR and data conversion

8.1.2 Responsibilities of the EHR-system

In the healthcare environment both the content of an EHR and rules for how to manage it are regulated at the national level. In many countries the service provider (e.g. hospital, health centre or GP) functions as a records authority and also has the responsibility for maintaining health records during their whole lifetime. So far as records are stored by the EHR-system, it has the responsibility of records management. The EHR-system can use ISO 15489-1 for internal records management.

The content of a health record is typically regulated by national legislation or by rules set by the Ministry of Health. The health professional, the user of the EHR-system, selects data objects to be captured with the "official health record". The EHR-system has the responsibility for support tools for this selection.

It is the task of the organization having the responsibility of managing EHRs (for example the hospital) to structure EHRs (using a data model supported by the eArchive) before they are sent to the eArchive. Organizations having the responsibility of managing EHRs (e.g. the data controller or a data producer) have the responsibility of:

— determining how long to retain the EHR;

— managing the meta-information of EHRs; this means that the record should include all metadata that are needed by the EHR-archive for long-term preservation and data disclosure;

— maintaining the classification of data objects of the EHR by security and purpose;

— maintaining the data structure of the EHR;

— managing necessary e-signature processes for proving the integrity and originality of EHRs;

— managing the registration of the EHR;

— putting the EHR into the data transfer structure that is accepted by the EHR-archive;

— performing risk identification and having a risk management system.

The EHR-system also has the responsibility of ensuring that the information transferred to the eArchive is "understandable"; that is, that users of the EHR can understand its information during the whole preservation time.

8.1.3 Shared responsibilities

If the EHR is a composite of separate parts created and managed by different organizations, the governance of the EHR itself may be either centralized or done by the "community" of service providers. In the case of a distributed EHR, a common method or cross-organizational system is needed for the management of the integrity and availability of the EHR.

The EHR-archive can be an external organization that offers archiving services for a group of health service producers. In this case EHRs will be transferred to the archive using a selected communication network. Both the EHR-system and the EHR-archive have a security policy and those polices will be bridged together. After that, both the eArchiving organization and the healthcare service organization together select a secure communication channel that meets national security and privacy protection requirements.

8.2 Policies

8.2.1 Archiving policy

It is necessary that the organization archiving health records (e.g. the EHR-archive) have a written archiving policy. The major elements of this policy are:

— archiving establishment policy including all operational tasks defined in 8.1.1;

— preservation policy-fulfilling national regulations;

— data discovery policy;

— data accessing policy;

— audit log preservation plan;

— data migration plan and migration control procedures;

— disaster recovery plan.

8.2.2 Security policy

The security policy means that the EHR-archive should preserve EHRs so that the confidentiality, availability and integrity of data and associated meta-information are maintained during the whole preservation time. Organizations archiving health records must create a written security policy document. The security policy is based on the risk analysis. Based on this analysis, criteria for acceptance of risks (for example following requirements set by ISO 27799) can be created.

8.2.3 Privacy protection policy

Privacy protection is a legal term and its requirements must be taken into consideration. In the healthcare domain, not only security but also privacy protection requirements must be defined and fulfilled. A comprehensive privacy protection policy is needed for the whole lifecycle of the EHR. A part of it is the privacy protection policy of the eArchive.

Basic principles for privacy protection are:

— data are not made available or disclosed to an unauthorized individual or computer process;

— data are not used in such a way that they harm an individual.

From the EU privacy protection directive and its implementation to national legislation, the following privacy protection requirements can be derived:

— IT-systems should be planned carefully in advance;

— a doctor-patient relationship or separate legislation is needed for data access (relationship principle);

— only those data that are necessary should be accessed;

— data cannot be used without patients' consent or specific legislation for purposes other than for which they have been collected (context and purpose tied utilization of data);

— there is a responsibility to inform the client of the use and disclosure of information.

9 Security and privacy protection architecture

Hardware and software technology supporting the eArchiving process is in many cases a combination of EHR-technology, telecommunication technology and digital archiving technology. It is necessary to develop common hardware and software architecture which makes it possible to fulfil security and privacy protection requirements. The practical implementation of this architecture might also need to be audited. If national regulations so stipulate, the architecture must also be certified.

10 Security and privacy protection requirements for the eArchiving process

10.1 Overview

The eArchiving process has been defined in this Technical Specification as a holistic process and it should meet ethical and legal requirements and good practice rules set by national authorities. During the creation

and management of the EHR-archive process, not only the present political and legal environment, but also all changes in the legal environment should be identified.

Figure 9 shows building blocks that can be used in creating security requirements for the archiving of EHRs.

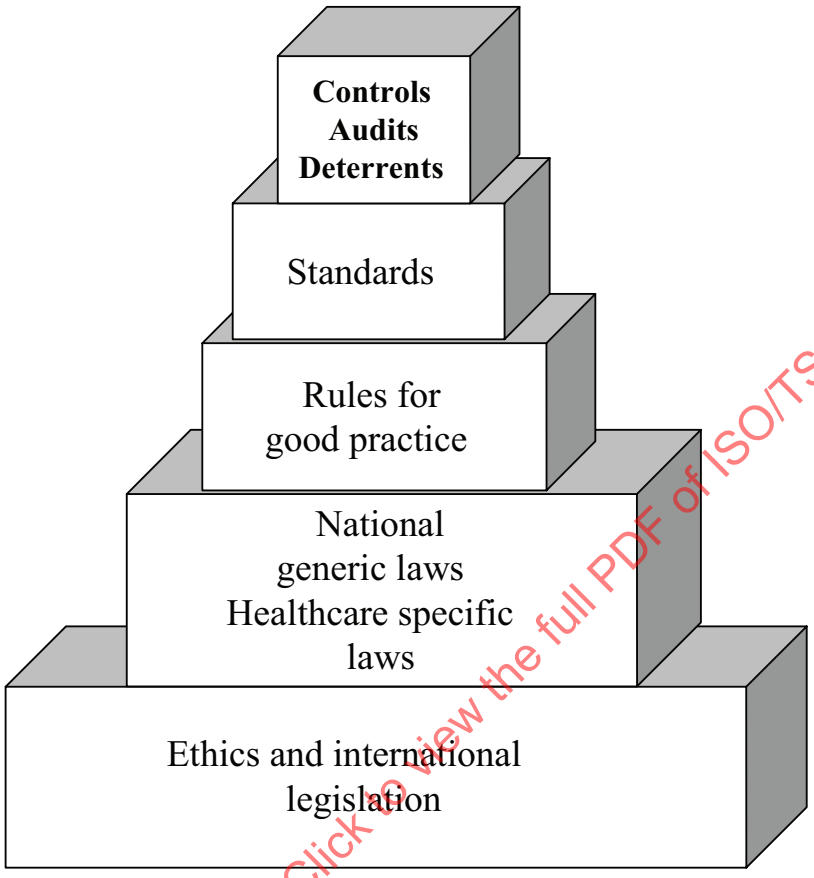

Figure 9 — Building blocks for the secure eArchiving process

A summary (checklist) of normative requirements defined in this chapter is shown in Annex F.

Both security requirements and security controls should be derived from the risk analysis of the whole eArchiving process. In the healthcare environment the risk analysis alone is not enough. Mandatory requirements set by legislation shall always be taken into consideration. ISO/TR 21548 shows a method by which this can be done in a controlled way.

10.2 Policies and responsibilities

All organizations participating in the eArchiving process of EHRs shall have a written:

— security policy;

— privacy protection policy;

— policy on data use and disclosure;

— archiving policy.

The security policy means that the EHR-archive should preserve health records so that the confidentiality, availability and integrity of data and associated meta-information is proven during the whole preservation period.

Policies should be bridged together in such a way that the entire eArchiving process offers the same level of security and privacy protection.

Practical implementation of the eArchiving system should fulfil requirements set by those policies.

The EHR-archive as well as the EHR-system should have the necessary administrative, physical and technical (e.g. access control, authentication, data encryption and systems for emergency access) infrastructure to ensure integrity, confidentiality, availability, accountability and privacy protection of stored data during the whole preservation period.

The responsibilities of all partners participating in the eArchiving process should be defined in a unique way.

The EHR-archive has the responsibility to check that necessary conditions for the disclosure of the EHR exist.

10.3 Requirements derived from legislation

10.3.1 Overview

Countries have different national legislation and rules for eArchiving (see Annexes A to D). From those rules, common security requirements have been derived for this Technical Specification. In addition, the EHR-archive implemented in any country should meet national regulations.

10.3.2 Preservation time of the health record

Health records (and their components) do have a normative defined preservation time. In practice, the preservation time ranges vary from a few years to more than a hundred years. Some countries have separate stipulations for permanent preservation of selected parts of patient records for scientific purposes. The preservation times for different types of records are determined by national regulations.

The EHR-archive (or the EHR-system) should evaluate the record; in other words, it should determine its preservation time already at the time of archival storage. This can be specified later if the regulations or needs change. The typical preservation categories include:

— short-term preservation (for example 1 y to 20 y);

— long-term preservation (for example during the patient's lifetime);

— permanent preservation.

The preservation time required is several decades. Even if EHRs were stored in an electronic archive with the status of notary archive, the archive will very probably have to perform both structural conversions and to resign the documents after the conversions by using the new organization key. Therefore it would be feasible to organize the long-term eArchive in such a way that there exists a trusted third party which can verify the archive as a notary archive.

10.3.3 Preservation of the original EHR

In many cases it is necessary to distinguish between the original EHR and its copies. Typically in the paper world the original record is a record signed by an authorized healthcare person (typically the responsible physician). In the case of digital records, the definition of the original record presents a problem even in cases where it comes with a time stamp and has been signed electronically. In some countries there is a policy to avoid copying of the records and to store the original record in one place (typically in the place of creation). If national legislation so stipulates, the original health record should be stored by the archive.

The eArchiving process should be defined in such a way that only one original EHR can exist and possible copies are marked to be copies. The copy information can be stored into the metadata of the record.

The archive should also have the necessary mechanism to prove the authenticity of original records. The person or organization responsible for preserving the original records shall be defined unambiguously.

10.3.4 Corrections and/or additions to the archived EHR

In most countries the national legislation regulates when and by whom it is possible to make corrections or update the EHR. It is typical that the content of the EHR cannot be changed after it is approved by the responsible health professional(s). In case of error, it is permitted to add information describing the reason for corrections. This process is managed by the organization responsible for the content of the EHR.

Typically the EHR-archive preserves health records in fixed format and the archive has to prove the integrity of the preserved record. Based on national regulations, corrections and additions to the record should typically be assigned to professionals authorized to make those corrections. In this case the new updated version of the record can be sent back to the archive for long-term preservation. It is necessary to mark the corrected version as being the most relevant for later use (e.g. for disclosure). It is also necessary for non-repudiation purposes to link the corrected and the uncorrected record and preserve them together. It might also be necessary to update the meta-information part of the record to show when and why corrections have been made.

Corrections and/additions made by the EHR-archive shall meet national regulations and norms and all corrections should be traceable.

10.3.5 Override conditions

In real life, situations exist where access is necessary, but the required patient consent cannot be obtained (e.g. to save a patient's life in a medical emergency situation).

If national legislation so stipulates, the access control of the archiving system shall accept this kind of access or data disclosure. Override situations shall be explicitly documented (for example, specifically labelled within the audit trail). Audit logs should be updated after this kind of data disclosure or access, and the patient should be informed afterwards of the reason for access.

10.3.6 Deletion of the EHR

Under special conditions the deletion of certain parts of the EHR can be allowed at the Court's request. In some instances the data can be ordered to be totally destroyed. The EHR-archive should have the necessary technical features to conduct this destruction and all events connected to deletion or destruction shall be marked in the audit log.

10.3.7 The nature of the health records

From a fixity point of view a health record can be:

— a static document where the form and content are recognised as substantially fixed throughout its lifecycle;

— a cumulative resource, whereby fixed parts are added to it throughout its lifecycle;

— a dynamic resource where the form and/or content change continuously or dynamically.

Archived EHRs are either static or cumulative resources. Based on national regulations the data of the EHR can have a juridical meaning only for a given period. Furthermore, the sensitivity of the EHR can change during its preservation time.

The EHR-archive should manage both the nature of the EHR and changes to the nature during the whole preservation time. This can be achieved by storing the nature and status information, of all objects of the EHR to the metadata and update its contents after any change.

10.3.8 Archival authority

In the healthcare domain, patient records typically have to be archived by a healthcare provider (e.g. hospital, healthcare centre) or by an independent medical doctor (GP or specialist). In many countries there is specific legislation or norms setting requirements for the archiving authority. Also in some cases health consumers (patients/clients) themselves can act as an archiving authority.

The archiving authority should maintain the eArchiving process in such a way that it fulfils all legal requirements.

10.3.9 Privacy protection and privacy of archived information

Organizations archiving health records should manage privacy protection based on national privacy protection legislation and healthcare-specific lower level regulations.

10.3.10 Consent management

National regulations and rules describe how patients can control the disclosure of their EHRs. In many cases, consent is required before the disclosure of an EHR or any of its objects. In some countries patients/citizens have the right to opt-in/opt-out of the record.

Because the archive has the responsibility of checking if conditions for the disclosure of the record exist and, if so, that these conditions are fulfilled, the EHR-archive should have the mechanism to check both the need and existence of the patient's consent before data disclosure. It is also possible that over time the patient can change his opinion about the sensitivity of his/her EHR. Therefore, the patient's consent should be checked before any data disclosure or access.

Patients' consent can be focused to affect only a part/section of the record. Therefore, the archive should have a mechanism to ensure that only the information matching the patients' consent is delivered (e.g. a data filtering service).

Since regulations may change over time and what is permissible or required to be disclosed may therefore change, the eArchive should store the history of consent and disclosure rules applicable to stored EHRs at each given time.

10.3.11 Protection of the EHR based on its purpose

The European Privacy Protection Directive and similar legislation in countries outside the EU define that personal data collected for one purpose cannot be used for other purposes without citizens' consent or specific national legislation.

The basic purpose for collecting patient information is to support the treatment plan for care to be given to the patient, the procedures performed on him/her and the respective examinations. There are also other purposes like proactive prevention, health summary for a driving licence and occupational care services. It is also possible that new purposes for use will arise during the EHR's lifecycle. The purpose of the parts/data objects of an EHR should be part of the meta-information of the EHR before the record is sent/moved to the archive.

The data transferred to the EHR-archive should contain necessary purpose information (e.g. classification). The metafile of the EHR should include information on the purpose for which data have been collected; and it might also contain additional information on other purposes for which the data can be used. The EHR-archive should have a mechanism to support purpose-based data access and disclosure. If the purpose of data use and the purpose defined in the access request do not match, the archive should reject the access (excluding situations where there is patient consent or an access is based on specific legislation).

10.3.12 Fine grain marking of objects

Different levels of protection are needed at different stages of the EHR-archiving lifecycle. It is not feasible to overprotect the document, since this is expensive and often makes the use of the document more difficult.

The EHR-system should mark data objects at selected granularity levels based both on the security and privacy protection needs, as well as the purpose and context of data objects. Preservation time should also be marked.

The access control system of the archive should manage the access of data objects at the finest granularity level based on the protection markings.

10.4 Requirements for availability

Long-term preservation of EHRs requires both long-term integrity and availability of the information. The preserved information should be both understandable and technically available to users during the whole preservation time. Increasingly it is also necessary that the data can be automatically processed without changing the meaning of the data.

If the data are stored only in presentation format, it is possible that later versions of application software cannot read or show the archived data correctly. Therefore it is a good practise to store both the presentation format and the plain text. Storing data in text format ensures better long-term preservation of records even if the presentation format could not be utilized towards the end of the document's lifecycle.

For short-term availability, the EHR-archive shall make regular backups.

Because file formats, software and platforms succeed each other rapidly, the EHR-archive should have a tested migration plan for safeguarding the availability of preserved records.

Patient records contain terms, classifications and codes that change over time. For health professionals, patients and other users, it is necessary to make the content of the EHR understandable (e.g. reach semantic interoperability) during the long preservation time. Therefore the EHR-archive should not only preserve the data but also information about terms, codes and classifications used in stored EHR. It is possible to use the metadata[3)] for this purpose.

Requirement 1: The EHR-archive must preserve information

In order for the preserved information to be both accessible and understandable for the customers needing it, even after a long period of time, information other than the actual data will also have to be stored. Therefore representation information, content information and preservation description information (e.g. metadata) should be archived in such a way that connections between the data, content, representation and preservation information cannot be broken during the preservation time (see Figure 10).

3) Metadata is a general name for descriptive information of documents and objects. It is information about information, describing the information content, explaining its meaning and how it can be used. Metadata are necessary for retrieval, use, security management and context specification of electronic documents. Using metadata facilitates information retrieval, automation of the handling of document drafting and document recording phases and creation of interconnections between different systems. It is critical that the accuracy of metadata is reliable.

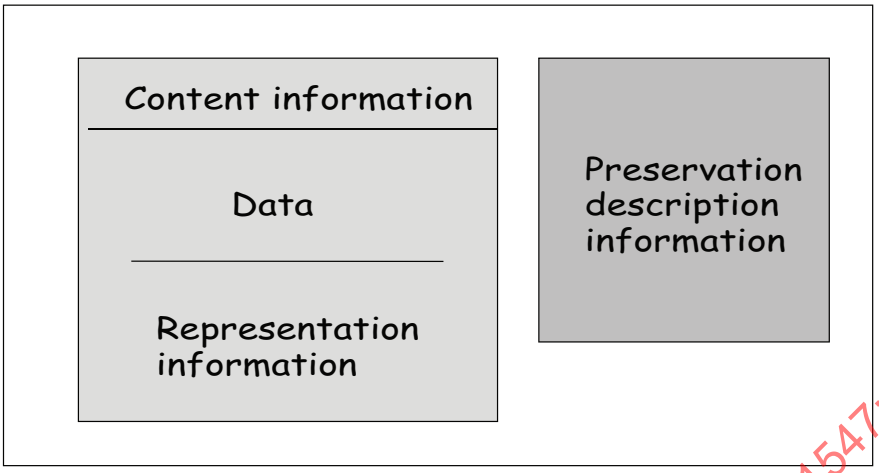

Figure 10 — ISO 14721 information model for the purpose of archiving

The metadata of the EHR should include semantic information about codes, terms and classifications used in the EHR. Another technical solution is to store definitions of all terms, codes and classifications in a separate "code server" and link definitions used in the EHR to this server. In this model it is not necessary to store information on terms, codes and classifications in the actual metadata of the EHR. The code server can be local, regional or even national.

The following healthcare example describes the relationship between components of the metadata (see Figure 10). A patient datasheet is typically expressed by characters representing the stored data. The characters are combined with the knowledge of the language used into meaningful information. The user of the information needs dictionary and grammar information to understand the text; in other words the representation information. The patient information contains results from a clinical laboratory (values). The content information includes information on how to understand these (e.g. reference values, the analysing method information, calibration values). The preservation description information includes a reference identifier by which the content information can be uniquely identified.

The health record itself has a contextual structure. Metadata describes the context and information content of the data and explains its meaning and the way to use the data. It also helps in information retrieval. From a security point of view the metadata includes information supporting availability, integrity, confidentiality and authenticity of the data.

The security part of the metadata typically includes the following information:

— identity of the creator of the data;

— sensitivity classification;

— legal obligations;

— retention time;

— purpose and context of the data collected;

— access restrictions and distribution rules.

Both the EHR and its metadata should be preserved as a whole. It is the task of the EHR system to create the necessary metadata. The role of the EHR-archive is to securely maintain this metadata and add meta-information (e.g. preservation description information) to the EHR needed for long-term preservation purposes.

The EHR-systems should add necessary security metadata to the metadata of the EHR before sending it to the EHR-archive.

The minimum content of metadata used in conjunction with the EHR can be defined by International Standards. One currently available metadata standard is the Dublin Core. In the case of transferring/storing EHRs in the form of documents the HL7 CDA R2 standard can be used. The CDA header is aimed at setting context for the document as a whole. It includes a "confidentiality code", which defines the overall confidentiality status of the document.

There are also other candidate metadata standards such as METS (metadata encoding and transmission standard) and MIX (metadata for images in XML standard). The header of HL7 CDA also includes meta-information that can be used for archiving purposes.

ISO 23081-1 defines the following security metadata:

— requirements about making available, reproducing or rendering records;

— access, use and retrieval rights and restrictions;

— time limitations to the access restrictions;

— regulatory requirements for record maintenance;

— security rules and polices;

— security classifications;

— retention time;

— integrity information;

— registration details.

The security metadata of the EHR should also include information about the confidentiality, purpose and context of the record.

Health records stored in the form of documents typically have a metadata part (e.g. a header) together with the body where the actual data are located. Metadata can also be stored as attributes of record objects (see EN 13606).

Requirement 2: The archive should find the requested information

The archive should have adequate data searching mechanisms and services.

The EHR should have a unique and consistent identification that expressly supports long-term preservation.

The EHR can be preserved as one fixed "packet" or it can be stored as a combination of fixed granular objects. Each object in the EHR can be connected to keywords (or headings). Those keywords can be stored at the metadata of the EHR. Keywords can be used by the archive for searching purposes. This kind of structure means that it is possible to search and find parts of the EHR based on the keywords.

Requirement 3: The EHR-archive should manage indexes, references and links

The EHR itself or its metadata can contain links to other records or external services (e.g. to a code/terminological server or a patient identification mapping service), references to other systems (e.g. knowledge bases) or guidelines as well as indexes that allow the grouping and naming of objects for the record. The EHR-archive should maintain those links and references in such a way that they cannot break during the preservation time thus proving the availability of the EHR as a whole.

The archive can also create links and indexes for internal availability. The EHR-archive should maintain the integrity of those links and indexes during the preservation time and prove that the migration process cannot change or break them.

Requirement 4: The EHR-archive should create and manage archival metadata connected to the EHR

The long-term preservation of EHRs for continued access requires additional archival metadata. This includes metadata about records management processes needed to support preservation, access, security, migration and conversion to ensure the accessibility of records and their authenticity, reliability, usability and integrity.

Typically the archive adds meta-information needed for long-term management of records/objects inside the EHR-archive to the received data. This archival metadata can be a separate metafile or the archive meta-information is added to the already existing metadata created by the EHR-system.

Any metadata that accompany the object when it is submitted to the archive must be verified and, as a necessity, enhanced to support the object's long-term maintenance. If the EHR-archive makes any change to the metadata of the EHR during the preservation period, changes should be audited and the archive should prove the non-repudiation of the metadata.

Requirement 5: The EHR-archive should have a method of restoring data to their former condition after any disturbance

This means that the EHR-archive should have a reliable backup system. It is necessary to test the backup system to prove that during restoration, no loss of data or meta-information takes place. It is also necessary to prove that links, pointers or indexes cannot be broken.

Requirement 6: The EHR-archive should support override conditions of data access

The access to a patient's EHR is always restricted based on national legislation and norms. In many cases the patient's consent is required for access. In some countries the patient can also opt-out of some part of their record. Cases exist (e.g. to save the patient's life) where it is necessary to override existing access restrictions. The EHR-archive should have a technology that allows the override of existing access rules when necessary.

All overriding activities should be audited and the reasons for overriding should be included in the audit log.

Requirement 7: The EHR shall be identified in a unique way

The unique identification of the EHR inside an archive is mandatory. It is good practice to identify every single record/document or object with an unambiguous identifier (ID) so that the identifier does not change during the lifecycle of the document. The identification is typically unambiguous within each organization, but it can also be unique at the national level. Additional identifiers can also be used for meaningful record objects (for example to separate record objects by the purpose of the data). It is also possible to use specific identifiers for some parts of a group of records (e.g. to use a separate ID for all data connected to the patient's service chain).

The EHR identifier cannot include information that reveals the identity of the patient or identifies his/her illness.

An electronic patient record can consist of several independent components, such as texts, multimedia images or sounds, each of which can get its own independent identifier. In this case all identifiers should be attached to the metadata of the EHR and linked together.

Within the document, different parts and objects can be identified in accordance with the OSI object model by means of object identifiers or line numbers thus making it possible to precisely refer to each section of the document.

The identifier can be globally or nationally unambiguous. The identifier of a document/record should remain unchanged throughout the entire lifecycle of the document. A record that has been modified will retain its original identifier, but the version number contained in the descriptive information will be updated and the

version history will be changed. When the preservation time expires, the EHR-archive should have the ability to destroy all independent parts of the EHR.

Requirement 8: The EHR and the subject of care shall be linked together in a unique way

The EHR-system managing electronic health records should uniquely identify both the service provider having the responsibility to create or update the EHR and the data subject, i.e. the patient (see ISO 27799). Based on requirement 7 the EHR shall have a unique identifier. Before the EHR is sent to the eArchive the EHR identifier and identification information of the subject of care shall be linked together uniquely by the service provider.

In many countries a unique patient or citizen identifier is used, but there are countries where it is not allowed to use unique patient identifiers. The patient identifier can be, for example, a pseudonym which is mapped to the subject of care. Depending upon national regulations, the mapping can be done at national, regional or even at service provider level.

Requirement 9: The EHR-archive should have a migration plan

In the healthcare environment the lifecycle of the EHR can be over a hundred years (see Figure 8). During this lifecycle, several applications and archive media will be used. Media conversions and/or structural conversions might have to be made as well. The migration plan is the tool to manage the availability of EHRs during their long preservation time. Therefore the EHR-archive should have a written data migration plan.

ISO/TR 18492 provides practical methodological guidance for the long-term preservation and retrieval of authentic electronic document-based information, when the retention period exceeds the expected life of the technology (hardware and software) used to create and maintain the information.

10.5 Requirements for integrity

The EHR-archive should maintain the integrity of stored information during the whole preservation time. To realize this, the EHR-archive:

1) has the responsibility for preservation of the original EHR during the whole preservation time;

2) should preserve both the data and associated metadata together as a whole;

3) shall have sufficient control over any modification and use of the stored information including possible modifications of the metadata;

4) should ensure that the EHR or any part of it is not destroyed (has not been destroyed) in an unauthorized way during its preservation time and/or in the case of EHR data communication;

5) should support a tamper-proof audit trail of all actions including data transfers;

6) should preserve and secure meta-information on the EHR and additional preservation information, as well as pointers and links against any unauthorized modification during the preservation time;

7) should manage both data encryption and decryption situations during the whole preservation period to maintain the integrity of preserved documents;

8) in the case of distributed EHRs (e.g. when the EHR contains links or references to other records or documents) the EHR-archive should maintain all pertinent links in such a way that broken or missing links cannot exist;

9) in the case of hybrid documents (e.g. document contains links to online documents) the archive should maintain all those links in such a way that broken or missing links cannot exist;

10) in the case where a common master index file/record links distributed EHRs together, the integrity of the master index file should be proven and any change in the master index file should be controlled and audited;

11) should only accept EHRs signed electronically by the doctor responsible or the EHR-system;

12) should ensure that EHRs disclosed by the system contain at least the signature of the EHR-archive (e.g. archival e-signature);

13) should manage the integrity of data in the case of any structural conversion needed during regulated preservation time.

An electronic signature is a widely used tool to prove the integrity of stored records. In healthcare a typical signer of the record before it is sent to the archive is a certified healthcare professional and the signature is a personal one. Sometimes more than one person has to sign the record. Depending on national legislation, information about the role of the signer is provided within the signature. The role information may contain both the professional status of the signer (for example specialist physician) and the job-related functional role describing their work task (for example assistant surgeon in internal medicine).

If legislation enables it, the signer of the EHR may also be an organization or its computer system. For example the archive can sign EHRs using “an organization e-signature”. A trusted EHR-archive (e.g. a notary EHR-archive) is an archive in which signatures have been verified by a trusted third party (TTP) and which have a certified non-repudiation service. Signatures made by the notary EHR-archive can have a similar legal value to personal signatures. One benefit of signatures made by the notary archive is that the signature key can be defined as having a much longer validity than a personal e-signature. National regulations permitting, the notary archive’s signature may replace the healthcare professional's signature.

If accepted by national legislation, the archive can also use “the archival e-signature” (e.g. soft signature) for the following purposes:

— verification of the integrity of the metafile and the integrity of the EHR's components;

— verification of the integrity of the stored EHRs after structural conversions;

— verification of the authenticity of a partial release of the EHR when the archive is releasing only a part extracted from the signed EHR;

— sealing of an EHR consisting of several parts into a digital envelope and verification of the integrity of the whole “archival packet”.

In case the archive converts the received signed EHR into another form for preservation purposes (for example from the form of display into an XML document), there is a danger of losing the non-repudiation of the signature made by the original record creator. This can be avoided if the archive is either a notary archive or it proves in another way that the content of the converted form is identical to the authentic one.

In the case of structural conversion during the preservation time, the content of the EHR should remain unchanged whereas the structure of the document is changed. When implementing a structural conversion, the old structure is retained. The archive verifies the validity of the change with an electronic signature. If needed for non-repudiation purposes, the converted document can retain the original identifier, but the version number is updated. The metadata of the EHR should also be updated and its version history should be preserved. In the case where the EHR contains both plain text and display format, both signatures should be available so far as a complete (100 %) conversion is impossible.

In the case of distributed EHR (records are archived in the place they are created), the maintenance of the integrity requires special attention. The integrity of each part of the EHR should be proved and there should be a mechanism to ensure that links and references cannot be broken. Typically links are stored in the metadata of the EHR. One commonly used solution stores links in a common master index record (e.g. regional or national). In this case the master index record should include information about all archived parts. The content

of the master index file should be synchronised in such a way that it contain online information of all archived parts of the virtual EHR. The management of the master index file should meet Requirement 3 in 10.4.

10.6 Requirements for confidentiality

To maintain confidentiality of archived EHRs during the preservation period and in connection with data disclosure, the following security requirements should be met.

1) The EHR-archive should ensure that data are not made available or disclosed to any unauthorized individual or computer process. The archive shall prevent unauthorized use of information and systems resources and therefore the archive shall control any kind of data disclosure and access.

2) The EHR-archive should have a mechanism to check any data access request against confidentiality information existing in the metadata of the record (for example confidentiality and/or sensitivity classifications, opt-out rules, purpose and context of the data).

3) The EHR-archive should maintain non-repudiation services so that the data origin is proven, no false sender or false data content exists and there is no false data receiver (person or computer system).

4) The EHR-archive should have a service for the accountability of archival events. The access control system has the responsibility to insist (and verify) that all actions of any data import and disclosure be checked.

5) The EHR-archive should have a mechanism to ensure that the connection between data and their metadata cannot be broken during the preservation, data disclosure and data migration.

6) The EHR-archive shall reliably identify all users, orders, producers and entities.

7) The EHR-archive should always check that all necessary conditions are met before it allows data access and disclosure.

8) The EHR-archive should monitor and audit all data access and disclosure.

9) The EHR-archive should have an access control system and in the case of direct access, it should manage privileges together with roles of users.

10) The EHR-archive should manage security policy bridging other organizations/service providers participating in the eArchiving process. This means that the archive should check that its own security policy and the security policy of the data requester and data producer are at a minimum at the same level.

11) The EHR-archive shall manage and update the audit log and store all preservation requests, access orders and disclose events.

12) The EHR-archive should have the ability to encrypt EHRs before data transfer or disclosure and, if needed, during the preservation time.

13) The EHR-archive should manage both the complete and partial delivery of information.

14) The EHR-archive should have controls against any malicious software (e.g. viruses, worms, Trojans, cookies) to prevent the corruption and/or loss of data.

15) The EHR-archive shall monitor and audit all changes in the EHR and metadata during structural conversions.

16) The archive always has the responsibility to check that all necessary conditions are met before it allows access to or transfer of the data. If the national regulations so stipulate, the data disclosed shall be marked on the patient's record.

17) An audit log shall include information about all use or disclosure requests sent to the archive. The audit log shall also include information to whom, when, for what purpose, and why the EHR or any part of it has been disclosed.

Rules and models for access control have been defined in ISO TC 215 Technical Secification “Privilege management and access control, Parts 1-3”. Therefore, this Technical Specification only summarises general principles for access to electronically archived patient records. Those principles are:

— a patient-doctor relationship is needed (the relationship principle);

— an acceptable reason to access is needed (medical ethics);

— access is given based on the needs arising in the care and treatment of the patient (the need to know principle):

  — only those professionals who are participating in the explicit care have permission to access;

  — managers and administrators have no permission to access;

  — patients have (in some circumstances) the right to restrict access;

  — there can be specific legislation to make access possible without the patient's consent (e.g. “in emergency cases to save life of patient”);

  — an ethical committee or official organization can give the access rights to a researcher;

  — secure authentication and identification of individuals and their roles is always needed within the specific domain.

In many countries the patient or citizen has the right to access their own health data. In some countries this is restricted. Before any access the patient/citizen should be identified in a trusted way (for example using smart cards and PKI-services).

In some countries the patient's consent is needed to access their personal health information across organizational boundaries.

In distributed EHR-archiving architectures where some parts of EHRs are moved from service provider level to national/regional level, the common repository should audit all information retrievals and accesses to distributed EHRs. The non-repudiation of this log should be proven and the log should be archived for a period defined by national legislation.

10.7 Requirement for non-repudiation

Non-repudiation has been traditionally defined as the inability to deny the integrity and authenticity of a document. From a communication point of view, non-repudiation means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively. In other words, non-repudiation of origin proves that data have been sent, and non-repudiation of delivery proves they have been received.[4)] Non-repudiation services typically include non-repudiation of origin, non-repudiation of delivery, non-repudiation of receipt, and non-repudiation of submission. The purpose of non-repudiation, in conformance with ISO/IEC 13888, is to provide verifiable proof or evidence recording of data.

4) Non-repudiation service provides proof of the integrity and origin of data (both in an unforgivable relationship) which can be verified by any party (ASTM).

Non-repudiation of origin. The principal receiving some data claims to know the data originator so that the sender cannot later deny having sent the data (HL7).

Non-repudiation of receipt. The principal sending some data claims to know that these data have successfully reached their intended receiver (HL7).

In its broader definition, non-repudiation means that there is undeniable evidence that a specific action has occurred.

The eArchiving process consists of a set of actions which all should be proven. Therefore non-repudiation in the case of eArchiving is more than just traceability or accountability.

In eArchiving of EHRs the non-repudiation services should include the following features:

— prove that the EHR has been signed;

— prove the submission of the EHR together with its metadata to the archive;

— prove the origin of EHR;

— prove that the EHR-archive has received the record;

— log all use, access and disclose events of stored EHRs and prove the time they occurred;

— prove that a data disclosure has occurred;

— prove who the receiver of the data is.

Non-repudiation services in eArchiving of EHRs should cover all events of the whole eArchiving process.

Non-repudiation service of the eArchive should create an audit-log including all events associated with the use, access and disclosure of the EHR.

Typically, the non-repudiation service generates an audit-record of all tracked events. A trusted time stamp can be included in this record to prove the time when the event occurred.

Electronic health records will have to be archived over long periods of time. The required lifecycle depends on national regulations, but typically the preservation time of patient information varies between 20 y and 100 y. The non-repudiation of stored information over these lengthy preservation periods needs to be fully proven, both to preclude loss and also to ensure that the ability to read and understand content is maintained. In most countries, the physician responsible should sign a patient's health record after the care or treatment episode. Their signature, together with a time stamp, proves not only the integrity of the data but also who has signed the record and in what role at a given time.

Electronic signatures, time stamps (e.g. e-signature of the time stamp CA), TTP services and event records are technologies used to reach non-repudiation. Based on the security limitations of available technology, it is possible that during the storage period digital signatures might become weak. Therefore, for long-term non-repudiation purposes, signature keys have to be refreshed periodically. It is a demanding task to build an EHR-archive supporting the non-repudiation of events. One possible solution to this problem is a trusted notary EHR-archive. It receives granular health data from different EHR-systems, stores data together with associated meta-information for long-periods and distributes granular EHR-data objects. It proves the non-repudiation of events and the integrity of stored data objects with the help of event records, archives time-stamps and archives e-signatures.

Annex A
(informative)

Framework for long-term archiving of EHRs in Finland

A.1 General

In Finland the EHR archived is the Regulated Record. Other parts of the health record, such as personal notes are not archived. EHRs are archived in the form of documents.

A.2 Legal and regulatory environment

The following legislation forms the umbrella for managing and using patient information.

EU-level regulation

— EU data protection directive;

— EU e-signature directive.

Generic national legislation

— Constitution of Finland;

— Data protecting in electronic communication (516/2004);

— Act relating to archiving (831/1994);

— Act relating to personal data protecting (523/1999);

— Criminal law;

— Act relating to services in the information society (458/2002);

— Act relating to electronic communication on the duty (13/2003);

— e-signature act (14/2003).

Healthcare-specific laws and decrees

— The law relating to patients' rights;

— Decree relating to the information entered into the patient's record (includes norms on the length of time documents should be preserved);

— Act relating to the management, use and archiving of electronic patient information (1.7.2007);

— Act relating to e-prescribing (1.7.2007);

— Decree relating to e-prescribing (225.6.2008);

— Decree relating to patient documents.

Standards

No formal decision exists to dictate which standards must be used, but at the national level the following standards have been proposed for use:

— HL7 CDA R2 (for eArchiving and EHR communication);

— HL7 R3 for e-prescriptions;

— DICOM (for images);

— JHS 143 (a national standard) for meta-information;

— XML/SOAP for communication;

— ISO/IEC 17799 and ISO 27799 for security management;

— ITU-T x. 500 and x. 509;

— ISO/TS 17090.

The following subjects will be covered as soon as the relevant International Standards are approved:

— ISO TC 215/WG4 *Privilege management and access control;*

— ISO TC 215/WG4 *Security requirements for archiving health records.*

A.3 Archiving

In Finland, archiving has a wider meaning than in Anglo-Saxon countries. In Finland archiving means a process that starts from the point of document creation and continues to the point where the document will be destroyed. The archiving covers the whole lifecycle of the document. For managing this archiving process every service provider organization should have a plan for establishing the archiving process (in Finland this plan has the name AMS). Figure A.1 shows the principles of the AMS.

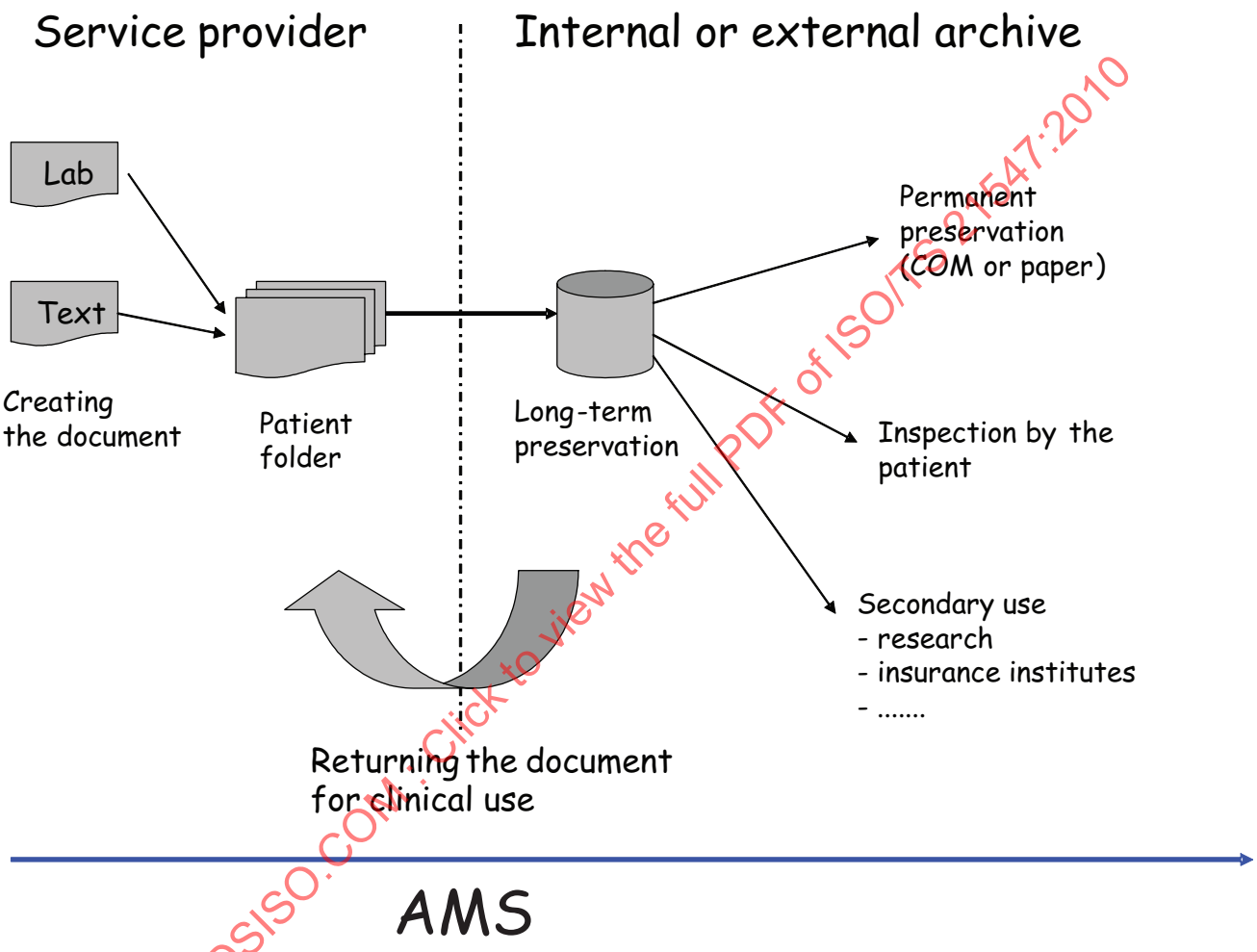

Figure A.1 — Principles of the Finnish AMSA.

Figure A.2 shows the proposed process view of an eArchive (source: Kansallinen sähköinen potilastietojen arkistopalvelu, "The National Archiving Services for EHRs, The Ministry of Social Affairs and Health 2005:21").

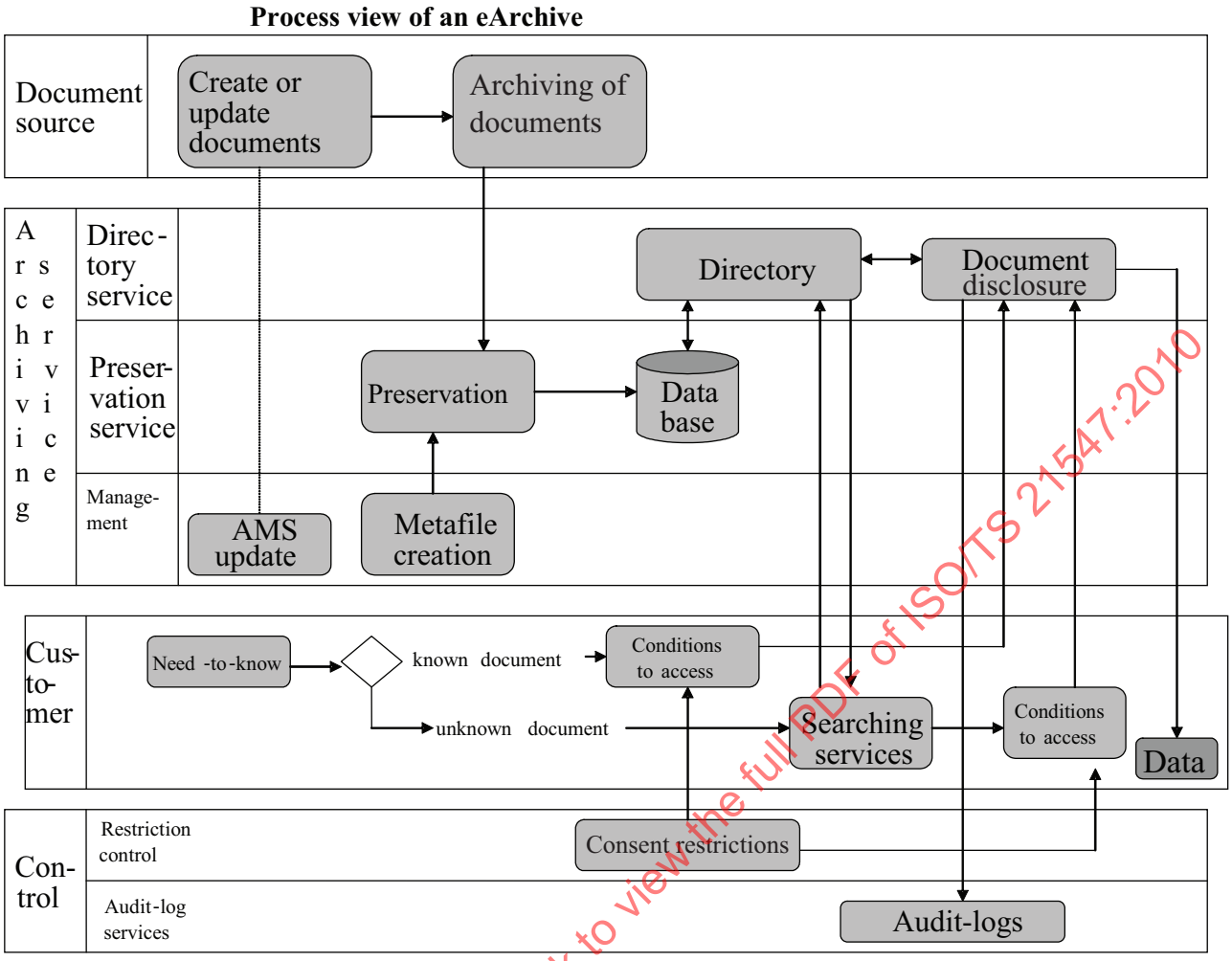

Figure A.2 — Process view of an eArchive

In Finland, health records are cumulative and life-long inside a service provider organization (i.e. secondary care hospital region, public healthcare centre, private service station/centre, occupational care service provider organization, or a private GP practice). Service providers have also the responsibility of archiving health records. Until now, most health records have been preserved in the form of paper records and archives are local independent archives.

In Finland the archiving period is quite long. Patient records with narrative text as well as EHRs can be destroyed 10 y after the death of the patient. Images will be preserved for 20 y. Up to 5 % of all health records should be archived permanently

A.4 National strategy for the management, use and disclosure of electronic health information

An updated national strategy (Principles on the National Healthcare Information System Architecture, Ministry of Social Affairs and Health 2006:8) stipulates that before the end of 2011 Finland will have one centralized eArchive for electronic healthcare and welfare documents. The act on the management and use of electronic patient information defines requirements, principles and rules for the use, management, archiving and disclosure of electronic health records.

Basic security and privacy protection requirements for the whole lifecycle of an EHR (including preservation) are:

— integrity;

— availability;

— accountability;

— confidentiality;

— long-term non-repudiation.

Figure A.3 shows how, in Finland, communication between a local EHR-system and the eArchive is planned.

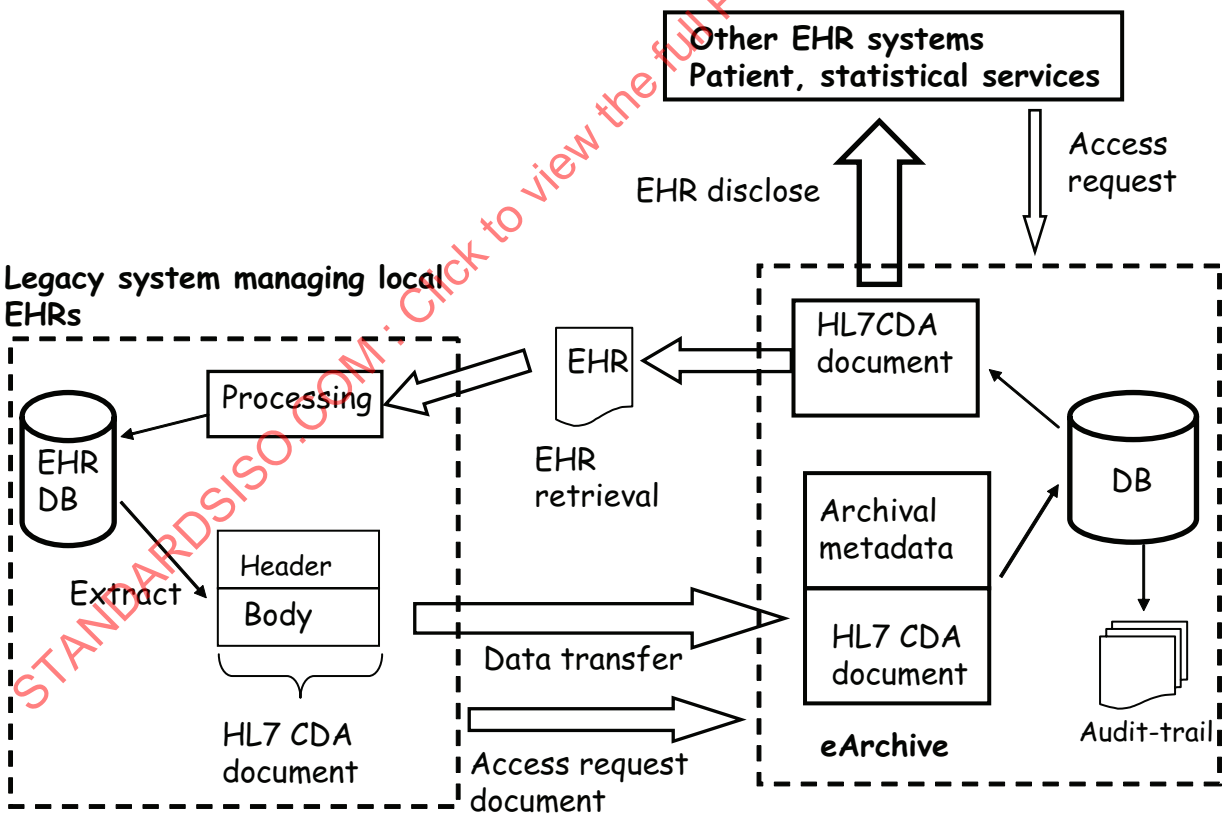

Figure A.3 — Finnish Model for EHR-system and eArchive communication

The act relating to the management and use of electronic patient information also sets the following requirements for eArchiving.

— Data transferred to the national eArchive shall have a nationally accepted structure.

— Patient information will be sent to the national eArchive, returned to the service provider or disclosed in the form of documents. Those documents should have a standardized metafile.

— The national eArchive can disclose patient records only in the case where the patient has given informed consent, or a specific law exists to allow the data disclosure.

— Any service provider asking for data disclosure should prove to the national eArchive that the care condition between the patient and service provider exists or the access is allowed by specific legislation.

— The citizen or patient has the right to know what data, to whom, when and for what purpose their records have been disclosed. The eArchive shall maintain a data disclosure log, which is accessible by the citizen via the Internet.

Annex B
(informative)

Framework for digital archiving of health records in the UK

B.1 General

The NHS has published two “Code of Practice” documents for health records:

— Health Record and Communication Practice Standards for Team Based Care;

— Records management: NHS Code of Practice (Confidentiality and Record Management).

The newest revision of NHS Code of Practice was published in the year 2006 (Records Management, NHS Code of Practice)[27].

B.2 Legal and regulatory environment

Legislation

A wide range of legislation exists in the UK. The following list consists of the most relevant legislation:

— Public Records Act 1958;

— The Access to Medical Reports Act 1988;

— The Data Protection Act 1988;

— Human Rights Act 1998.

Rights are qualified rights; this means that in certain circumstances they can be set aside by the state: national security, protection of public safety, protection of health or morals, prevention of crime or disorder, protection of the economic well-being of the country, and protection of the rights and freedoms of others.

— The Access to Health Records Act 1990;

— The Census (Confidentiality) Act 1991;

— The Common Law Duty of Confidentiality;

— The Data Protection (Processing of Sensitive Personal Data) Order 2000;

— The Freedom of Information Act 2000;

— Electronic Communication Act 2000;

— Administrative Law;

— The Health and Social Care Act 2001.

The Common Law Duty of Confidentiality is not written out in one document like an Act of Parliament. It is case law.

Guidelines

— HSC 1999/053 Managing Records in NHS Trusts and Health Authorities – for the record;

— NHS Retention & Disposal Schedule – for the record;

— HSG(96)18, The Protection and Use of Patient Information, Department of Health Guidance on Confidentiality;

— Report on the Review of Patient-Identifiable Information, Caldicott Committee 1997;

— HSC 1998/089 Implementing the Recommendations of the Caldicott Report;

— HSC 1999/012 Caldicott Guardians;

— HSC 1998/217 Preservation, Retention and Destruction of GP General Medical Service Records Relating to Patients;

— ECL 2/68 Disposal of Records which have Lost their Value;

— HSC 1998/153 Using Electronic Records in Hospital: Legal Requirements and Good Practice;

— Hospital Patient Case Records - A Guide to their Retention and Disposal, the Health Archives Group's Booklet;

— HSG (95)3, Health Service Use of Ionising Radiation;

— Confidentiality, NHS Code of Practice, 2003;

— Records Management, NHS Code of Practice, Part 1 and Part 2, 2006.

Standards mentioned

NHS Code of Practice [27] includes a list of useful standards. International standards mentioned in this list are:

— ISO/IEC 17799;

— ISO 15489-1;

— ISO 19005-1;

— XML.

B.3 Records management policy in the UK

In this context “The Record” has the following definition:

“structured document, which contains information (in any form) and which has been created or gathered as a result of any aspect of the work of NHS employees.”

Health Service Circular (HSC 1999/053) has been published to improve the management of NHS records in Health Authorities and Trusts.

It:

— sets out the legal obligations for all NHS bodies to keep proper records;

— provides guidelines on good practice;

— lists suggested minimum periods for retention of records.

The circular recommends that NHS Trust and Health authorities should draw up a records management strategy so that records are properly controlled, readily accessible and available for use and archived or otherwise disposed. Many health trusts have established a records management policy. This policy consists of the following topics:

— legal obligation and good practice;

— confidentiality and data protection;

— general principles;

— creating records;

— principles of efficient storage;

— disposal of unwanted records.

A policy document “e-Government Policy Framework for Electronic Records Management” (2001) emphasises the following.

— Privacy and access issues, and particularly freedom of information legislation, require that electronic records be managed consistently within regulatory frameworks. Aspects of electronic records management should be built into both record-generating and records management systems to ensure that these longer-term requirements are met by constructing interactive systems of software, standards, policies, procedures and interfaces.

— The longer term requirements of public records will require public sector organizations to plan for the migration of records, as hardware and software platforms change, to ensure continued access and authenticity.

— Records must be subject to more stringent controls, such as prevention of content alternation and allocation of schedules for retention and disposal.

— Cross-government standards for metadata.

In this policy framework, the requirements of good electronic record-keeping have been defined as follows:

— good understanding of the nature of records, and the electronic information that should be captured as records;

— the process of capturing records should be easy and understandable to use;

— electronic record-keeping systems are designed to manage reliable and authentic records, ensuring that the integrity and reliability of records is secured;

— a strategy to ensure that records will remain accessible and usable for as long as they are needed;

— the ability to apply appropriate appraisal, scheduling and disposal procedures to manage records.

From privacy and data sharing points of view the need for authentication, auditing, e-signatures and time stamps are mentioned.

B.4 Records management

NHS Code of Practice [27] gives a framework and requirements for NHS record management, preservation and archiving. It uses the following definitions.

Authenticity: an authentic record is one that can be proven to be what it purports to be, to have been created or sent by the person purported to have created or sent it and to have been created or sent at the time purported.

Destruction: the process of eliminating or deleting records beyond any possible reconstruction (see ISO 15489-1).

Disposal: the implementation of appraisal and review decisions.

Disposition: a range of processes associated with implementing record retention, destruction or transfer decisions which are documented by disposition authorities. There are two principal options: to dispose (e.g. by passing on to another organization) or to destroy.

Permanent retention: records may not ordinarily be retained for more than 30 y. The Public Records Act provides for records that are still in current use to be legally retained. Under separate legislation, records may need to be retained for longer than 30 y.

Preservation: process and operations involved in ensuring the technical and intellectual survival of authentic records through time.

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

Record system/Record-keeping system: an information system that captures, manages and provides access to records through time.

Retention: the continued storage and maintenance of records for as long as they are required.

Weeding: the process of removing inactive/non-current health records from the active/current or primary records storage area to a designated secondary storage area on a locally agreed time scale after the date of last entry in the record.

The above describes the required standards of practice in the management of records for work within or under contract to NHS organizations in the United Kingdom. It covers NHS patients treated on the behalf of the NHS in the private healthcare sector. This code of practice identifies the specific actions, managerial responsibilities, and minimum retention periods for the effective management of NHS records.

Types of record covered by the Code of Practice include: patient health records, operating theatre records, accident, emergency and birth registers and administrative records.

General context

All NHS records are public records under the terms of the Public Records Act. All NHS organizations have a duty to make arrangements for the safe keeping and eventual disposal of all types of record. The Keeper of Public Records (answerable to Parliament) gives overall guidance and supervision. The National Archives is the body that is responsible for advising on the management of public records. The National Archives has general oversight of the arrangements for permanent preservation of records in local records offices, which have been formally approved by them as Places of Deposit.

Chief executives and senior management of all NHS organizations are personally accountable for records management within their organization. Individuals who work for an NHS organization are responsible for any records that they create in the performance of their duties. Those records are public records.

Personal data are defined as data relating to a living individual, which enables him/her to be identified either from those data alone or from those data in conjunction with other information in the data controller's possession.

Processing includes everything done with that information. Using includes disposal (i.e. closure of the record), transfer to an archive or destruction of the record.

The aims of NHS records management are:

— to maintain an information governance framework in relation to the creation, use, storage, management and disposal of records;

— to clarify legal obligations and explain actions required to fulfil these obligations;

— to explain the requirement to select records for permanent preservation;

— to set out the recommended minimum period for retention.

NHS Code of Practice defines the following management and organizational responsibilities:

— the records management function should be recognised as a specific corporative responsibility within every NHS organization.

— a designated member of staff of appropriate seniority should have lead responsibility for records management within the organization

— each NHS organization should have in place an overall statement on how it manages all of its records. These policy statements should define roles and responsibilities within the organization. It should provide standards, procedures and guidelines.

The code of practice defines the following requirements.

Record creation: records of operational activities should be complete and accurate to allow appropriate actions in the context of their responsibilities, to facilitate an audit, and to protect the legal rights of the organization, its patients, staff and other people affecting by its actions, and provide authentication of the records so that the evidence derived from the records is shown to be credible and authoritative.

Record-keeping: the record-keeping system should include a documented set of rules for referencing, titling, indexing and, if appropriate, protective marking of records.

Record maintenance: the movement and location of records should be controlled and there should be an auditable trail of records transactions. Backup and planned migration to new platforms should be designed and scheduled. Equipment use for stored records should provide storage that is safe from unauthorized access. A contingency or business continuity plan should be in place to provide protection for all types of record.

Disclosure and transfer of records: there is a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties and ranges of provisions that require or permit disclose (see B.2, Caldicott Guardians). Mechanisms for transferring records from one organization to another should be tailored to the sensitivity of the material.

Retention and disposal arrangements: part two of the Code of Practice includes guidance on retention periods. The disposal of records should be undertaken in clearly established policies.

Appraisal of records: appraisal refers to the process of determining whether records are worthy of permanent archival processing. Most records, even administrative ones, contain sensitive or confidential information. It is vital that confidentiality be safeguarded at every stage of the lifecycle of the record.

Record closure: records should be closed (i.e. made inactive and transferred to secondary storage) as soon as they have ceased to be in active use other than for reference purposes. An indication that a folder of electronic records has been closed should be shown on the record itself as well as noted in the index or database of the folders. Where possible, information on the intended disposal of electronic records should be included in the metadata when the record is created.

Record disposal: each organization should have a retention/disposal policy. Records not selected for archival preservation should be destroyed in as secure a manner as possible. It is the responsibility of the NHS organization to ensure that methods used throughout the destruction process provide adequate safeguards against the accidental loss or disclosure of the contents of the records. A record of the destruction of records should be maintained and preserved by the records manager.

Electronic records management (ERM) supports the medium- to long-term information management needs of the business. It provides a digital environment for capturing electronic documents and applying standard records practices. The ERM system must preserve content, structure and context of the electronic records, and must ensure that records are “registered” and that authentication procedures and an audit trail are put in place (to permit these records to be used as legal evidence). Typical requirements for electronic records management are to support:

— capturing, storing, indexing and retrieving all elements of the record as a complex unit;

— management of records within class categories or filing structures to maintain the narrative links between records;

— record level metadata including retention and disposal rules;

— integration between electronic and paper records;

— secure storage and management to ensure authenticity and accountability including support for legal and regulatory requirements – preventing change of content;

— appraisal and selection of records for preservation and transfer;

— management facilities for systematic retention and disposal of records;

— migration and export records for permanent preservation without loss of information.

Based on UK documents, general requirements for electronic document management systems are:

— document capture policy;

— storage and indexing should be done at the document level;

— search and retrieval should be done at the document level;

— access management and security control service are needed;

— version control;

— audit trails on access and changes of the document should be maintained;

— document profiles (information about the document) should be created.

B.5 Data protection principles

Personal data shall be processed fairly and lawfully. Relevant conditions to process health records are:

— where the processing is necessary to protect the vital interest of the patient;

— with the (explicit) consent of the patient;

— where the processing is necessary to protect another person;

— for medical purposes by a health professional;

Personal data are not processed in a way that is incompatible with the purpose for which they were obtained. Patients should be fully informed about the reason why their information is required. If information is obtained for a specific purpose, it must not be used for anything else unless consent is obtained for other uses of the information. For example, identifiable patient information gathered to provide healthcare cannot be used for research unless consent is obtained or the information is anonymised.

It is the right of individuals to seek access to their records held by the health or social care provider.

Under the common law, a healthcare provider wishing to disclose a patient's personal information to anyone outside the team providing care should first seek the consent of that patient. It is not the easy way to override consent using the public interest principle. Solid justification is required.

Employees should only have access to those parts of the record required to carry out their role. Requests for record access by other staff members should be logged and periodically audited.

B.6 Archives

The Code of Practice uses the following definition.

Archives are those records that are appraised as having permanent value for evidence of ongoing rights or obligations, for historical or statistical research or as part of the corporate memory of an organization.

Generally an EHR can be stored in the local information system (online system) for 30 y. It is also possible to move an inactive record to secondary storage for long-term preservation purposes. After an appraisal procedure, records can be transferred to a permanent archive. This means that records selected for archival preservation and longer in regular use by the organization, should be transferred as soon as possible to an archival institution (for example a place of deposit). Non-active records should be transferred no later than from creation of the record [27].

It is also a legal requirement that NHS records which have been selected as archives should be held in a repository that has been approved for the purpose by the National Archives.

In the UK archiving has been understood (in a very traditional way) to be a permanent preservation of selected records that are transferred to a repository (place of deposit) approved for this purpose by the National Archives. Records management includes the systematic control of the creation, receipt, maintenance, use and disposition of records in a primary or secondary storage.

B.7 NHS Care Record Service

NHS Connecting for Health (NHS CFH) is working to ensure that all NHS patient records will be kept in electronic format. An NHS number has been adopted as the unique identifier for all patient records. The NHS Care Record System Review Group has made a recommendation that, in the UK, there are two "records": Summary Care Record and Detailed Care Record.

The Summary Care Record will have the following features:

— initially populated with key historical data from GP systems;

— updated as significant problems or prescriptions occur;

— available to clinicians with a legitimate relationship to the patient;

— important diagnoses, procedures, allergies, inter-actions and recent prescriptions;

— patient can limit their participation.

It is recommended that the Summary Care Record be continuously uploaded with GP and hospital information, including sensitive information that requires consent.

Access control will be based on roles and legitimate relationships. Auditing and policing is also required.

Annex C
(informative)

Framework for digital archiving of health records in Japan

C.1 Legal and regulatory environment

C.1.1 Legislation

— Personal Information Protection (Privacy) law (2003);

— E-Document law (2005).

C.1.2 Guidelines

— safety management guideline for healthcare information systems (Ministry of Health, Labour and Welfare 2005) (includes requirements for electronic preservation, outside preservation of health records and related records, electronic preservation of health records with scanner and deployment);

— an additional guideline is under development (JAHIS/Security Committee Electronic Preservation Working Group);

— guideline for applicable treatment of personal information in healthcare (hospital-related associations).

C.1.3 General security requirements

— authenticity;

— readability;

— resolvability;

— confidentiality.

C.2 Other security features included/mentioned

C.2.1 General

— access control;

— user authentication;

— backup;

— recovery procedures;

— confidentiality;

— accountability (in the case of outside preservation);

— responsible creator of the record;

— emergency case access;

— access by approved person;

— act confirmation (in the case of communication);

— audit trail;

— outsourcing;

— patient objections;

— interoperability;

— responsibility;

— anti-virus measures.

C.2.2 Specific safeguards mentioned

— encryption;

— E-signature;

— time Stamp;

— WORM-technology for long-term preservation.

C.2.3 Standards mentioned

— ISO 19005-1 (PDF/A long-term preservation format);

— ISO 14721 (OAIS reference model);

— ISO 15489-1 (records management);

— ISO/TR 15801 (trustworthiness);

— JIS Z 6016.

From Figure C.1, we can deduce that in relation to the OAIS model there are overlaps between ISO 14721 and other ISO records management standards used in Japan.

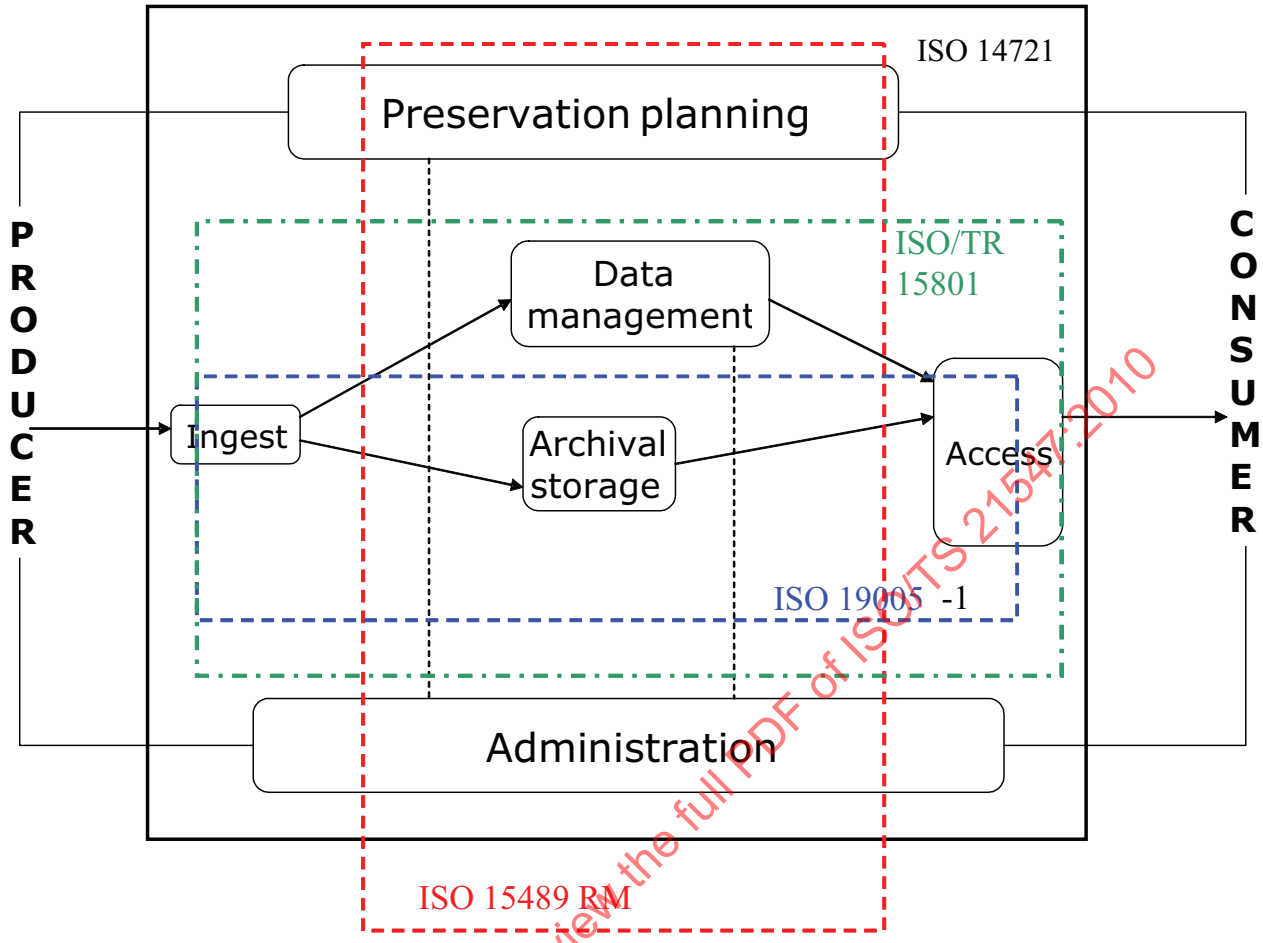

Figure C.1 — Overlap between ISO standards and OAIS-model[5)]

From the picture we can derive, that in relation to the OAIS- model:

— ISO 15489-1 covers administration, archival storage and preservation planning;

— ISO 19005-1 covers ingest, access and archival storage;

— ISO/TR 15801 covers data management, ingest, archival storage and access.

5) Ingest is an OIAS entity that contains services and functions that accept submission information packages from producers and prepares archival information packages for storage (see ISO 14721). Figure C.1 is courtesy of Mr. H. Hasegawa.

Annex D
(informative)

Framework for digital archiving of health records in the USA — Rules and requirements derived from HIPAA

The regulatory environment in the USA is very heterogeneous. There are over 10 000 federal, state and local laws and regulations addressing what, how, when and why records must be created, stored, accessed, maintained and retained over longer periods over time.

Definition:

The eArchive is a system for storing the fixed content of data with associated metadata and policies.

The content of the record is defined automatically before it is sent to the archive. After the file is archived, it cannot be modified or deleted before its preservation time expires.

Typical information stored by the eArchive is:

— electronic health records;

— the billing record;

— doctor's authorization documents;

— all information connected to the communication between patient and doctor.

Rules and requirements derived from the HIPAA Act in the domain of eArchiving are:

— an eArchive should have a security policy;

— information should be kept secure and confidential during the preservation time;

— the service provider has the responsibility for preservation;

— an eArchive should have a centralized monitoring and control system;

— audit documents should be stored for a minimum of 7 y;

— an archiving organization should have an administrative and technical infrastructure to ensure confidentiality and integrity;

— it is necessary to control who is using information to avoid errors, and control any data change;

— the eArchive should have necessary administrative, physical and technical safeguards to maintain data access (e.g. access control services), data integrity and encryption;

— the eArchive should have administrative and technical facilities for the emergency access of data;

— the eArchive should have a data discovery policy:

  — the eArchive should maintain a repository with meta-information which describes the nature of the document, where and when it was created and by whom;

- the eArchive should have a security and data protection policy:
  - only authorized users have the right to access;
  - activity logging – audit trails are required (including history of the document, change history and access history);
  - regular audit trail analysis is required;
- a centralized eArchive can store information from many different sources;
- the eArchive should have a regulatory compliance policy;
- rules concerning the data structure are:
  - data will be stored using fixed data content;
  - fine grain definition of fixed data;
  - data and metadata forms an object;
  - object is capsulated;
  - objects should be marked by their content;
  - objects cannot be altered during the preservation time;
  - each object should have a metafile;
  - the metafile should include policies connected to the object;
  - the archive should support multiple levels of data protection;
- the archiving period should be included in the metafile;
- metadata should make it possible to manage different document types in different ways.

HIPAA administrative safeguards:

- Security management:
  - risk analysis;
  - risk management;
  - sanction policy;
  - activity review.
- Personnel security management:
  - authorization;
  - termination of employment.

- Information access management:
  - access control services.
- Security awareness:
  - education;
  - virus control;
  - log-in monitoring;
  - user management and privilege management.
- Contingency plan:
  - backup plan;
  - disaster plan;
  - emergency mode operation plan.
- Business/contracts:
  - management of contracts.
- Physical safeguards:
  - access control of facilities;
  - security of workstations;
  - data backup.
- Technical safeguards:
  - unique identification of users;
  - emergency access procedure;
  - decryption services;
  - automatic user logoff:
    - audit control;
    - data integrity;
    - secure communication lines.

Annex E
(informative)

Comparison of ISO 15489-1 and ISO/TS 21547 security requirements for archiving of electronic health records

ISO 15489-1	ISO/TS 21547
Definitions: **Records management** Field of management responsible for efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.	**Definitions:** **Archive** An organization that intends to preserve information for access and use for any designed users or process (OAIS Red Book, June 12, 2001). Electronic archive (EHR-archive) preserves information in digital format. It is an information system that receives, manages and provides access to records through their whole lifecycle. **Archiving process** A holistic long-term process covering the whole lifecycle of the health record. **Archiving** is a combination of data reception management, data preservation and access management, security and privacy protection management, records management, information description methods, and storage media technology.
Policy Organizations should define and document policies for records management. Organizations should ensure that policy is implemented at all levels in the organization.	**Policy** Organizations archiving health records shall have a written archiving policy. Organizations archiving personal health information shall have a written security policy document. The EHR-archive should have a privacy protection policy.
	Elements of the EHR-archive Definition used is based on the ISO 14721, reference model for open archival information systems.
	Types of the EHR-archive Definition of different types.
	eArchiving process eArchiving is a holistic process covering the whole lifecycle of the EHR. During preservation time health records are dynamic.
	eArchiving process and records management From an eArchiving process point of view both ISO 15489-1 and this Technical Specification can be used together.

ISO 15489-1	ISO/TS 21547
	Environment of the eArchive Producer. Customer.
Responsibilities It should be clear who is responsible. Responsibilities should be assigned. Specific leadership responsibility should be assigned to a person with appropriate authority within an organization (e.g. records management professionals, executives, systems administrators, employees). Archival authorities may be involved.	**Responsibilities** Electronic archiving of health records is a holistic process between data producers, customers and the EHR-archive. Responsibilities of all partners should be defined. List of basic responsibilities for an EHR-archive. List of operational responsibilities. Responsibilities for long-term preservation. The EHR-archive has the responsibility to maintain the technical usability of the stored record.
	Security and privacy protection architecture
Records management requirements To support the continuing conduct of business and comply with the regulatory environment, it is necessary to maintain: – accountability; – reliability and authenticity; – usable and reliable records; – integrity protection.	**Security and privacy protection requirements for the eArchiving process** The eArchiving process should meet ethical and legal requirements and good practice rules set by national authorities. The EHR-archive should have the necessary administrative, physical and technical (access control, authentication, data encryption and systems for emergency access) infrastructure to ensure integrity, confidentiality, availability, accountability and privacy protection of stored data during the whole preservation period. The EHR-archive must preserve information. The archive should find the requested information. The EHR-archive should manage indexes, references and links. The EHR-archive should manage archived metafile information and data description information. The EHR-archive should have a method of restoring data to its former condition after any disturbance. The EHR-archive should support override conditions of data access. Unique identifying of electronic patient records. The EHR identifier and identification information of the subject of care shall be linked together uniquely by the service provider. Creators of the EHR should be reliable, identified and authorized. Migration plan. Non-repudiation management. Preservation time management. Responsibility for preservation of the original document. Corrections and/or additions to the archived documents. Overriding condition management.