TECHNICAL REPORT

ISO/TR 21548

First edition
2010-02-01

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

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

Reference number
ISO/TR 21548:2010(E)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

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

Introduction

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

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

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

1 Scope

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

2 Terms and definitions

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

3 Abbreviated terms

— CDA Clinical documentation architecture

— EHR Electronic health record

— GP General practitioner

— HIS Hospital information system

— HL7 Health level 7

— ISMS Information security management system

— PKI Public Key Infrastructure

— LAN Local area network

— PACS Picture Archiving and Communication System

— TTP Trusted Third Party

— XML Extensible Mark-up Language

— VPN Virtual Private Network

4 eArchive and eArchiving process

4.1 eArchive

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

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

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

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

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

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

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

4.2 eArchiving process

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

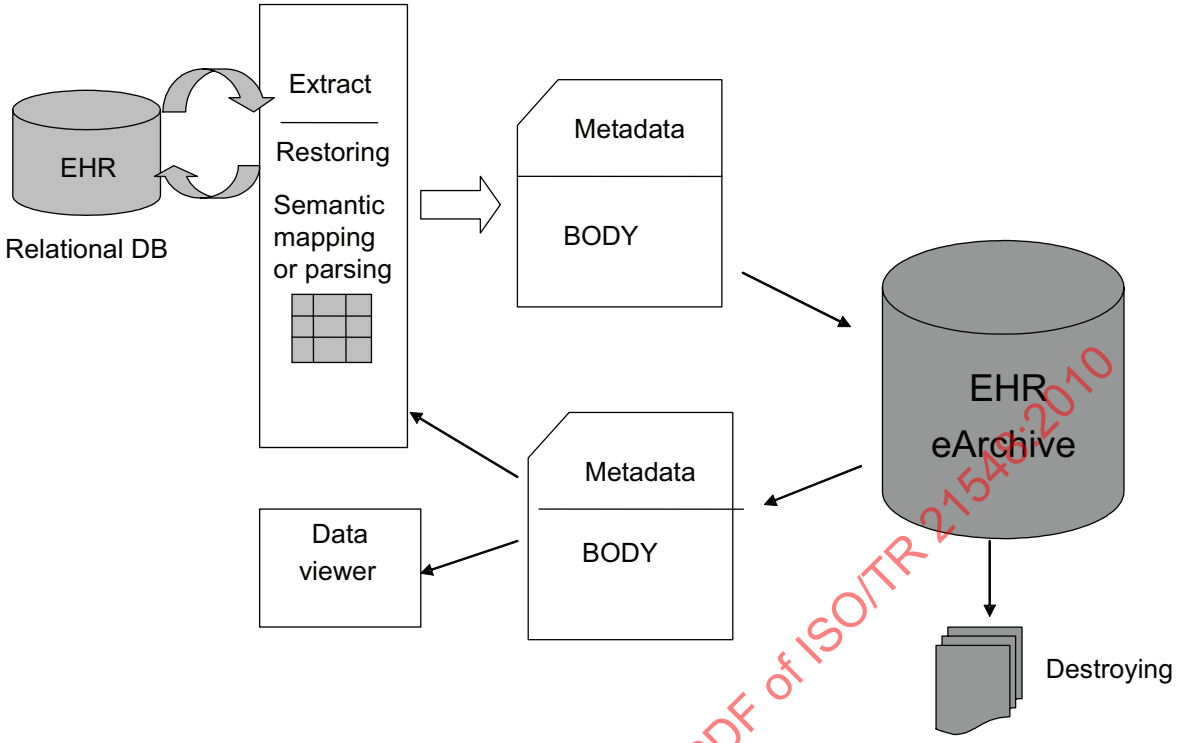

Figure 1 — Example of the eArchiving process

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

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

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

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

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

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

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

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

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

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

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

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

— security services needed to view and restore disclosed data;

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

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

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

4.3 Backup and recovery

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

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

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

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

5 Environment of the eArchive

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

6 Responsibilities and policies

6.1 General

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

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

— archiving policy;

— security policy;

— privacy protection policy.

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

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

This Technical Report provides additional guidance on those policies.

6.2 Responsibilities

6.2.1 Introduction

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

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

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

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

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

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

6.2.2 Responsibilities of the eArchive

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

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

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

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

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

6.2.3 Responsibilities of the EHR system

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

— who has control responsibilities for the management of EHRs;

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

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

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

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

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

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

— patient consent information;

— information about the purpose of requested data;

— definition of acts and norms that enable data disclosure;

— information needed to enable the overriding condition.

6.2.4 Shared responsibilities

Communication between the eArchive and the EHR system should be trustworthy. Typically, the requisite telecommunication services are bought from a third party (e.g. tele-operator). Before signing a contract both the eArchive and the service provider should:

— analyse existing legislation, security norms and rules;

— perform a risk analysis,

— select the required security level;

— define to whom, when and how the network operator should communicate the details of security events or any potential security and data protection incidents.

It is the responsibility of the telecommunication service provider to prove that health records are not made available to any unauthorized person, process or entity during the data transmission. It should also prove the integrity of data. There exists a wide selection of technologies for these purposes, such as data encryption, electronic envelopes, secure communication lines and protocols (e.g. VPN and SSL).

Trusted communication means that all partners have been identified and authenticated uniquely. Both mutual authentication and certification services offered by a trusted third party can be deployed to assure trust.

6.3 Policies

6.3.1 Overview

The eArchive is designed to receive, maintain, store, disclose and destroy electronic health records with the help of automated computer processes. This means that software used by the eArchive should meet requirements derived from archiving, security and data protection policies. This can be realised by deriving rules from policies and using policy languages for implementation of those rules.

The archive can receive health records from different sources, and records creators can have different security and privacy protection policies. Therefore the archive should always be concurrent and compliant with those policies relevant to the received information. This can be realised by:

— including necessary policy information to the metafile of the archival data packet (ISO 23081-1);

— an automatic negotiation process between the EHR system and the eArchive;

— including policy information to the contract regulating the eArchiving process.

The eArchive and the whole eArchiving process should be audited and/or certified to meet policies.

6.3.2 Archiving policy

ISO/TS 21547 defines that the eArchive should have a written archiving policy. The policy should be derived from an analysis of the eArchiving business plan (ISO 15489-1). It should meet requirements set by legislation, norms, standards and best practice rules.

It is necessary that not only the eArchive, but also the whole eArchiving process have a comprehensive eArchiving policy. ISO/TS 21547 defines major elements of this policy document.

The archiving policy document should be accepted by all partners to the eArchiving process, documented and published.

6.3.3 Security policy

ISO/IEC 17799 and ISO 27799 define general security requirements for the management of health information. However, those International Standards do not address specific problems arising when EHRs are archived. The aim of this Technical Report is to give additional guidelines for the secure eArchiving process.

Organizations archiving personal health information shall have a written security policy document. It is proposed that this policy is based on requirements set by ISO/IEC 17799 and ISO 27799. The security policy should cover the entire eArchiving process. The policy should be derived from the results of the risk analysis of the eArchiving process. The security policy should meet requirements set by national legislation, norms, standards and best practice rules.

The security policy document should be accepted by all partners to the eArchiving process, documented and published.

Because the eArchive can preserve health records having differing/varying security requirements, the security policy of the eArchive should define principles to preserve, disclose and destroy stored EHRs according to their security policy.

6.3.4 Privacy protection policy

Privacy protection legislation defines the rights and duties of organizations and people with respect to the processing of personal data. Processing covers the entire lifecycle of personal data from creation to destruction. Basic privacy protection principles are universal. The EU Personal Data Protection Act has defined seven principles. Those principles focusing on the long-term archiving of health records are shown in Table 1[1)].

The eArchive shall have a privacy protection policy. The main target of this policy is to protect patient privacy and also verify that patients can exercise their rights (e.g. inspect their own health data) in accordance with agreed procedures. This policy should meet requirements set by national (and/or international) legislation, norms and guidelines (e.g. HIPAA-legislation, Act on patient rights, EC Data Protection Directive). Table 1 can be used as the starting point to formulate the privacy protection policy for long term archiving of electronic health records.

The privacy protection policy document should be accepted by all partners to the eArchiving process, documented and published.

The privacy protection policy should define how conflicts about privacy policies of partners of the eArchiving process are resolved and settled.

1) Source: Privacy-Enhancing Technologies, White paper, the Dutch Ministry of the Interior and Kingdom Relations.

Table 1 — Summary of privacy protection principles for eArchiving of health records

Privacy protection principle	Application to eArchiving of health records
Transparency	The patient must be informed about health organizations and reasons for processing his or her health data. The patient must be informed about the rules to exercise his or her consent and opt-out rights.
Justification	The health data can be used only for purposes for which they are collected. No further processing or the use of data for other purposes is allowed without informed consent or specific national legislation. Basic purpose to process health data is to organize care and/or treatment. Not all data collected by a health person or organization is aimed solely for care or treatment. Therefore the data should be marked by their purpose before they are sent to the eArchive.
Legitimate grounds	National and international legislations regulate and restrict who, when and why health records can be processed. They also restrict the transfer of health data to countries which do not set out adequate privacy rules. The eArchiving process must meet national privacy protection regulations. Regulatory and legal frameworks in different countries can provide varying degrees of protection of privacy, and the "adequacy" of protection can remain open to interpretation. Companies offering eArchiving services must comply with the regulations of countries in which they operate. They should also inform clients of the impact those regulations may have upon the level of security and privacy protection of EHRs they store on behalf of those clients. The outsourcing decision should be based on business needs and risk assessments. Generally, the EHR-archive cannot be outsourced to companies that cannot guarantee adequate privacy protection of archived EHRs.
Quality	Collected health data should be relevant and proportional to the processing purposes, accurate and not kept longer than necessary. Preservation periods are typically regulated at national level. The data sent to the eArchive shall include preservation period information. The eArchive should destroy a record when its preservation period ends.
Rights of the patient	These rights are based on national legislation. The patient can exercise his consent or opt-out privileges to prevent the eArchiving or disclosure of any record. The eArchive shall check patient opt-out or consent before any EHR disclosure.
Security	The partners of the eArchiving process should take all necessary technical and organizational precautions to safeguard EHRs from loss or against any form of unlawful processing. This Technical Report, ISO 27799 and ISO 15489-1 are targeted both to underpin the security requirements and to provide the tools for secure archiving of health records

7 Design and implementation of secure eArchiving process for EHRs

7.1 General discussion

Most EHR systems in use are not specified for secure long-term preservation of health records. They are, predominantly, online systems targeted to support local workflows in the conduct and administration of direct care. During the care process, the patient EHR may be updated many times daily by many people, computer systems or applications. Typical security services implemented at a legacy systems level are: identification of users, privilege management and access control services, systems logs, back-up and/or replication services. Some systems may also have the ability to "close" the record at a point in the care period in such a way that it is no longer possible to change the content of the record.

In healthcare the traditional archive is paper-storage, but dedicated electronic archives also exist (e.g. PACS for digitalized images). Because online EHR systems are not planned for secure long-term preservation of health records, they in most cases do not fulfil all security requirements needed for long term eArchiving of EHRs. However, when designing and implementing a secure eArchiving process, the presence of legacy EHR systems and their functionality should be taken into consideration.

It is theoretically possible to develop an EHR system having the ability to archive health records securely without requiring a separate eArchive. Such a system can prove the non-repudiation of any event occurring during the lifetime of the computer system, and can also restore any state of the EHR occurring during its lifetime. Whichever type of system is used, online systems archiving health records should meet security requirements defined by this Technical Report and national legislation.

ISO/TR 15489-2 sets out a generic model for the design and implementation of records systems. ISO 27799 proposes use of the concept of an information security management system (ISMS) as a starting point. Merging those two models, the following nine-step model can be used for the design and development of a secure eArchiving process:

Step A: Understand the environment of the eArchiving process, together with the administrative, legal, business and social contexts in which it operates.

Step B: Analyse business activity and develop a conceptual model that sets out what each organization participating in the eArchiving process does and how.

Step C: Assess existing EHR systems and eArchives, and the security services they support.

Step D: Identify existing security requirements for eArchiving of EHRs. This includes requirements set by legislation and International Standards (e.g. this Technical Report, ISO 27799 and ISO 15489-1).

Step E: Perform a risk analysis covering the whole eArchiving process. This step includes both planning the risk analysis and performing it systematically.

Step F: Create strategies to satisfy security requirements. This includes the creation of policies and the selection of security safeguards and tools. Contracts with other partners and vendors should also be completed at this stage.

Step G: Design the eArchiving process and the eArchive. This step includes all necessary changes to the current security services of EHR systems, together with any processes and changes to the content or structure of the EHR (if needed).

Step H: Implement eArchiving service and processes. This includes the implementation of selected security and privacy protection services.

Step I: Conduct a post-implementation review. This includes security audits and, if required, security certification of the entire eArchiving process.

7.2 Analysis of the business model

The purpose of the business model is to develop a map showing what the eArchiving process and its partners (e.g. the eArchive, EHR system and third parties) do and how. This model includes a definition of methods by which EHRs are prepared for archiving, sent or received to the archive and distributed in a secure way. The business model includes identification and classification of organizations participating in both the eArchiving process and the classification of customers. The business model should identify both the model of the eArchive which is or will be implemented and its means of communication with EHR systems and customers.

One part of the business model is to define the purpose of the eArchive itself. The business model can be for example:

— long-term preservation of legally defined EHRs;

— acting as a notary archive for long-term preservations of all kinds of healthcare documents;

— archiving only fixed health documents (e.g. the whole EHR or set of fixed objects);

— an online electronic storage archiving active multimedia records;

— a permanent repository for EHRs.

7.3 Identification of impact of ethical and legal requirements

The eArchive should meet ethical principles and legal requirements set by international societal norms and national legislation. The archive should therefore identify those requirements. In more practical terms, it should model tasks and processes of the archive and identify at each step:

— from where health records are received;

— which data are processed and by whom;

— security requirements connected to the record and its elements;

— legal and ethical requirements concerning data processing in all steps;

— for what purposes the EHR is processed;

— which data are transferred to the archive.

Findings of this kind of analysis can be used both for risk analysis and for defining the privilege levels required for data access.

The main ethical principles to take into account are:

— patient-clinician relationship, needed for access (the relationship principle);

— only those professionals who are participating in the explicit care process have privileges to access the EHR;

— an acceptable reason to access is needed;

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

Those principles mean that before responding to a request for any data disclosure the eArchive should ensure that acceptable reason exists and the application or person requesting data disclosure from the eArchive has an appropriate right to access the required data.

7.4 Risk analysis of existing systems and the developed system

ISO/TS 21547 states that the eArchive should both analyse risks and have a risk management mechanism.

An eArchive can be a new service connected to existing EHR systems. It is necessary to perform a holistic risk analysis including all components of the eArchiving process (e.g. including network operators/operations) and prove that all components fulfil security requirements.

The eArchive operates over many decades and during this period new EHR systems will be connected to it. It is necessary to perform the risk analysis in advance as a part of the development of those systems before they are connected to the archive.

Both ISO/IEC 27001 and ISO/IEC 13335-3 define the components of risk analysis. Those International Standards and ISO 27799 can be used as a starting point for the risk analysis.

ISO/IEC 15408 (which describes the common criteria or CC) is a widely used multipart International Standard aimed at the development of products and systems with IT security functions or systems and the procurement of commercial products and systems with such functions. ISO/IEC 15408 addresses protection of information from unauthorized disclosure, modification or loss of use. ISO/IEC 15408 can be used for the evaluation of security of EHR archiving systems.

8 Implementation of security requirements

ISO/TS 21547 has defined a comprehensive set of security requirements for long-term preservation of EHRs. However, the implementation should always meet requirements set by national legislation, norms and ethical codes. In practice this means that national regulations, norms or guidelines can limit or even restrict the implementation of some requirements defined in this Technical Report.

Figure 2 describes a four-layer model that can be used as a tool in generating domain or platform-specific rules from the generic requirements defined in ISO/TS 21547. The use of this model fulfils realised tasks defined in step D of Clause 7.

The layers have the following meanings.

— The layer of generic requirements includes security requirements set by ISO/TS 21547 and is interconnected to other International Standards.

— The layer of national filtering includes all enablers and restriction derived from national legislation, norms and rules.

— The system level layer describes the actual platform of the planned or implemented eArchiving system. The processes, activities and tasks of the eArchiving system should be described. In this level the data flow between processes and acts should be fully described.

— The lowest level includes all available security services and tools. The level of security or trust each service or tool offers should be defined or described.

Use of this model requires that security requirements should be defined for each process or activity described at system level. Those specific system requirements are derived from general requirements and filtered through national level rules which can allow, restrict or limit the use of generic requirements.

The final task is to define security tools, safeguards and services which together offer the selected level of trust for the whole eArchiving process. Clause 9 describes how those tools can be selected with the help of risk analysis.

Table 2 shows how it is possible to link the nine-step development model of a secure eArchiving process (see Clause 7) and this security implementation model.

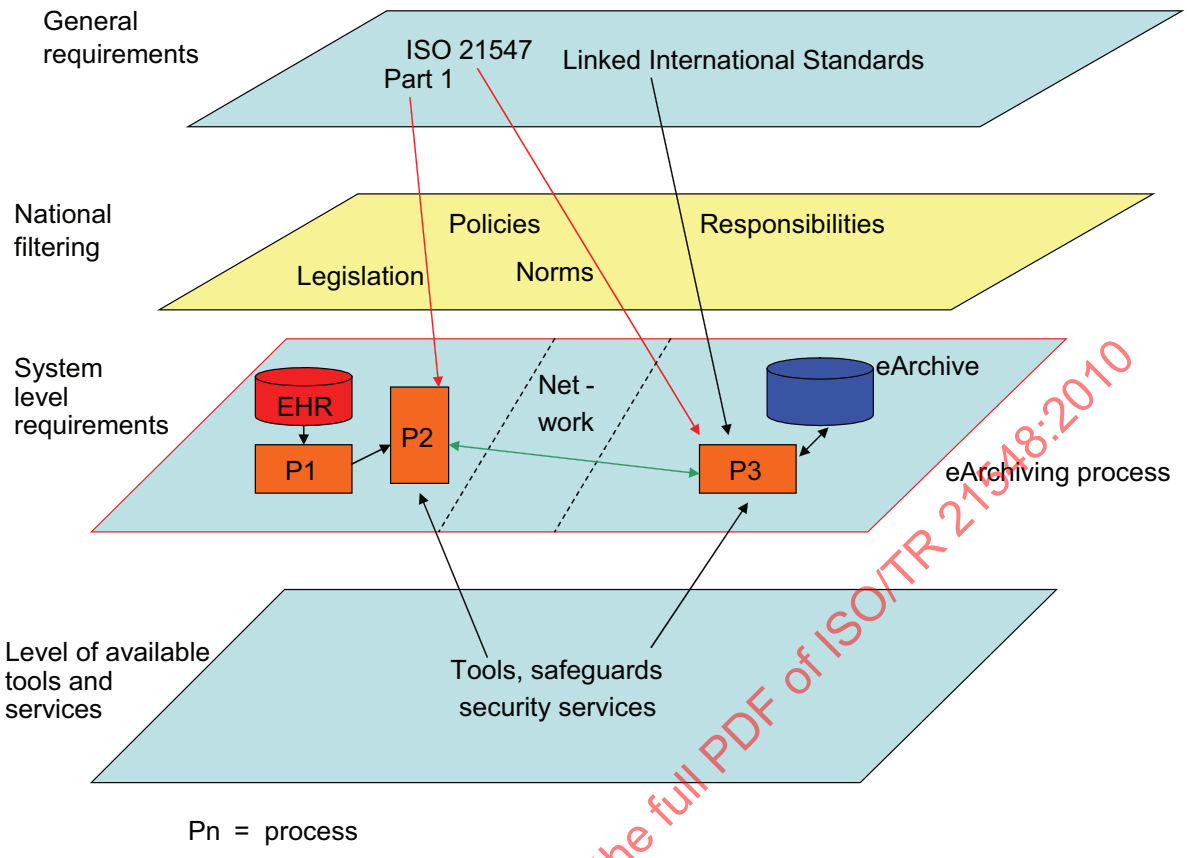

Figure 2 — Four layer model for implementation of security requirements

Table 2 — Connection between eArchiving process and security implementation models

Model phases (Clause 7)	**Layers** (from Figure 2)
Step A	Generic requirements National filtering System level
Step B	System level
Step C	System level Tools and services
Step D	Generic requirements National filtering
Step E	All layers
Step F	National filtering System level
Step G	System level Tools and services
Step H	System level Tools and services
Step I	All layers

9 Security and privacy protection controls and instruments for archiving of EHRs

9.1 Tasks of the eArchive

ISO 14721:2003, Annex F, has developed a functional reference model for open archival systems. ISO/TS 21547 has used this model as a reference for defining tasks of the EHR archive.

The basic tasks of an eArchive are the following.

a) Receiving and handling the request for data preservation, including the following tasks:

- identifying the data producer (e.g. EHR system);
- receiving records in accepted standard formats;
- checking data and metadata integrity;
- checking malware, etc.;
- updating audit logs;
- sending a receipt to the data producer.

b) Preparing received instructions/directions for preservation, including the following tasks:

- managing data transformations to match the preservation format;
- formulating the archival metafile;
- updating archival index files and pointers;
- securing data integrity (e.g. by using archival e-signature);
- encrypting data (if necessary);
- including protection that preserved records can be linked to only one person.

c) Preservation of EHRs and preservation management, including the following tasks:

- managing data migration;
- EHR back-up;
- storing the record and connected metadata as defined in the preservation policy;
- disaster management.

d) Ensuring the long-term availability of records, including the following tasks:

- registering records stored by the archive;
- managing semantic interoperability (storing and making available the meaning of terms, classifications, codes and vocabulary used in a particular record);
- managing index tables/files, key words;
- supporting different terminals (GSM, VPN, Internet etc.).

e) Receiving and managing access requests from customers, including the following tasks:

- identifying customers (health organization, health person or patient);
- checking that legal and other necessary conditions for the access or record disclose exist;
- managing patient consent and opt-outs;
- collecting required records or record components from technical storage of the eArchive;
- managing data format transformations (if needed);
- securing data integrity (e.g. signing the record using archival e-signature).

f) Data disclosure and access, including the following tasks:

- selecting a secure transmission method/channel;
- transmitting data;
- in the case of end users having access to online archived health records, the archive should manage the privilege levels and access permissions of those persons;
- receiving a receipt from customer;
- updating audit logs.

g) Special administrative functions, including the following tasks:

- managing access permissions of information officers controlling the functions of the eArchive;
- managing the partial delivery of data;
- managing integrity in case of partial delivery;
- managing access needs in emergency cases;
- long-term non-repudiation of all activities.

Based on the analysis of tasks a) to g) and the associated risk analysis, it is possible to define the organizational functions and technical instruments required to meet the security requirements.

9.2 Tasks of EHR system

The main tasks of the EHR system using preservation services offered by the eArchive are:

- entering health information to the EHR-database in such a semantic and technical structure that meets requirements for long-term interoperability and comprehension;
- extracting health records targeted for archiving from the database of the EHR system;
- mapping terms and classifications from internal presentation to the presentations required for interoperability (if needed);
- creating the security metadata required by the archive;
- creating the archival information package (AIP) and securing its integrity;

— creating and sending the preservation request to the archive;

— creating security documents as consent and relationship documents (if needed);

— sending the AIP together with security documents to the archive;

— creating the data disclosure request to the archive, or activating an online access process;

— receiving records from the eArchive;

— updating the audit-log.

9.3 Selection of security instruments

The definition of security requirements for an eArchiving system is described in Clause 8. Using this method, security requirements can be set for any process, task or activity of the practical eArchiving system. For the practical implementation, it is also necessary to select the set of security safeguards, tools and services which together prove the selected level of trust and security and minimise security risks. Figure 3 shows this process.

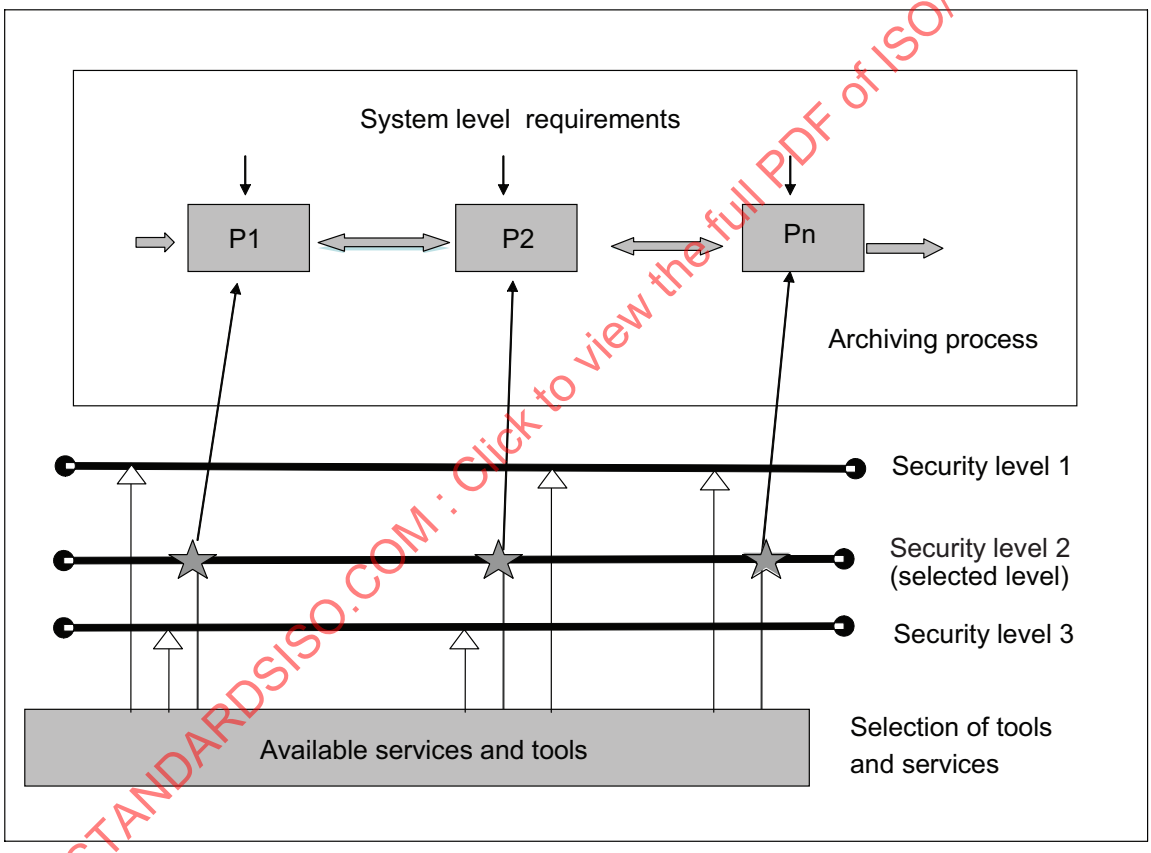

Figure 3 — Selection of security tools

The eArchiving process consists of a set of tasks described in 9.1 and 9.2. Security risks should also be analysed for each of those processes (see Clause 7). Based on security requirements set out in ISO/TS 21547 and the risk analysis, it possible to define the security level needed.

In practice, different security instruments offer different levels of security and for any task there are many technical instruments available, offering varying levels of security. Some of those instruments can provide a very high security level, but on the other hand they can be very expensive to implement and also impractical to use.

After the selection of the trust and security level needed for the entire eArchiving process, security tools used for different tasks and activities can be selected in such a way that they all offer the same (optimum) level of security (see Figure 3).

9.4 Privacy protection instruments

Whilst security instruments can be used to prevent the unauthorized access of health data (an important component of privacy) they do not equal privacy protection. “Privacy Enhancing Technologies” (PET) have been available for the last ten years. Typical PET tools are:

— authentication and authorization tools;

— identity protectors as pseudonymization and anonymity tools;

— biometric access control tools;

— federated identity management systems;

— firewalls;

— encryption tools;

— digital watermarks.

ISO/TS 21547 has defined security protection requirements necessary for long term archiving of EHRs. When correctly applied, those security controls and tools fulfilling those requirements also have privacy enhancing functions and no additional privacy protection instruments are required.

All participants in the eArchiving process should determine whether any privacy protection situations should be deployed where selected security tools are not sufficient.

9.5 Audit-log

The audit trail is an instrument which is used for confidentiality, availability and privacy protection. Organizations participating in the eArchiving process should maintain the complete audit trail in order to allow traceability of the use and disclosure of the EHR.

The ISO/TC 215 WG 4 work item on audit trails for electronic health records is producing a full ISO International Standard for audit trails. This International Standard can be used for audit logs needed in the eArchiving process.

9.6 Security instruments

9.6.1 General

Requirements for security are defined in Clause 10 of ISO/TS 21547:—.

An eArchive should protect confidentiality, integrity, availability and accountability of health records when accessed and throughout the entire preservation period. Non-repudiation of stored records over these lengthy preservation periods needs to be fully proven.

All necessary administrative measures, together with the physical and technical infrastructure, and the security instruments to ensure confidentiality, integrity and availability should be selected and implemented. The selection of a security instrument is part of steps F and H in the model defined in Clause 7.

Instruments required for secure archiving of health records are both administrative and technical. Typical security instruments available for digital archiving of health records are:

— authentication;

— signing of records and associated metadata for integrity;

— encryption of records;

— audit-logs;

— archive timestamps;

— event records for non-repudiation;

— privilege management and access control services (e.g. RBAC systems);

— PKI services;

— digital timestamps for authenticity;

— security metadata, including: context, purpose, confidentiality and sensitivity classification;

— term and classification repositories for long-term availability;

— obligation repositories.

Long-term preservation of electronic health records is a demanding task. The useful lifetime of stored health information in many cases exceeds the lifespan of formats and technical tools used for security (e.g. it is possible that during the storage period the validity of some digital signatures may become weakened, and PKI-certificates might be revoked or expire). Therefore such types of security instrument should be selected with long-term usability in mind.

It is the responsibility of health organizations and the eArchive to select the combination of security instruments that match the security level defined for the long-term archiving of EHRs.

9.6.2 Availability instruments

9.6.2.1 General

The eArchive has the responsibility of making information available in a correct and independently understandable form throughout its regulated preservation time.

Instruments for availability include:

— archival information model (e.g. ISO 14721 model);

— metadata;

— terminological, classification and vocabulary services for long term usability of preserved information;

— index terms for the retrieval of data objects across classification, categories and media; indexing can be automatically generated by electronic profiles (ISO/TR 15489-2);

— retrieval service having the ability to use metadata, links and indexes and make it possible to have different views to the archived data;

— standards for communication and long term preservation as DICOM, PDF/A, HL7 CDA and XML.

— software for the management of overriding conditions. Overriding conditions in healthcare are typically defined by legislation (for example overriding opt-out and patient consent is allowed to save the life of the patient). The implemented access control system of the archive should support the possibility of accessing the patient record overriding normal access rules. Overriding access cases should always be audited.

9.6.2.2 Instrument for short term availability

Strategies for short-term availability include copying and combining different kinds of hardware and software technologies. Copying is the production of an identical copy within the same medium. Electronic copies (e.g. back-ups) can also be done on different kinds of electronic medium:

— back-ups and copies can be used to enable disaster recovery of the archived information;

— replication can also be used for short term availability;

— hardware solutions, as storage arrays, can be used for short term availability.

9.6.2.3 Instruments for long term availability

Health records should be archived for decades. It is a demanding task to maintain both the semantic and technical availability of EHRs. During the preservation time, the meaning of terms and classification can change. Both software and hardware changes are required. Data formats and standards will also change.

Migration plan and technical migration services are key instruments for long term availability of records. They should cover all the necessary software and hardware changes needed throughout the whole preservation period.

The key instruments for the technical migration are migration services and conversions. Migration services include tasks designed to periodically transfer digital material from one hardware/software configuration to another. Conversion involves a change of the format of the record but ensures that the primary information (content) of the record remains identical. Migration plan and conversions should form part of the archiving policy (ISO/TR 15489-2).

The migration process should be documented and tested in advance.

A typical instrument for long-term semantic availability and usability is a term and code repository that stores the history of all terms, classifications and codes used in the EHR. If terms and codes used in the EHR are linked to the content of the repository, it is possible to know the meaning of terms and codes at the time they were used. Another possibility is to embed the semantic information of used terms into the structure of the preserved record.

9.6.3 Integrity instruments

The integrity of a record is typically secured by using an electronic signature mechanism. A typical signer of the EHR is a certified healthcare professional and the signature is a personal one. Information about the role of the professional is usually provided within the signature. The role information may contain both the professional status of the signer (for example medical doctor) and the job-related dynamic role describing his work task (for example responsible healthcare professional).

If the record is converted into another form from the display form before signing it (for example into an XML document) the signature application shall be audited prior to its implementation. This is done to ensure that the professional who has signed the document can be certain that the stored information is identical to the display that he has signed in good faith.

In structural conversion the content of a record should remain unchanged whereas the structure of the document is changed. When implementing a structural conversion, the old structure is retained. The initiator of the conversion verifies the validity of the change with an electronic signature. The corrected document will retain the original identifier, but the version number contained in the meta-information is updated and the version history is changed. The original document containing plain text and original signatures must be available insofar as a complete (100 %) conversion is impossible.

The signer may also be an organization or the computer system. The eArchive can use this kind of technical e-signature to sign the archival information packet (e.g. using an “archival e-signature”). Technically this kind of signature is a software signature. If a trusted third party verifies the archive and the archival signature process, the archive acts as a “notary” archive. One benefit of the notary archive and the use of an archival e-signature is that the signature key used can provide much longer validity than traditional personal e-signature keys can. This means that there will be less need for the refreshing of keys.

National regulations permitting a signature by the notary archive may replace the signature of a healthcare professional.

The eArchive can use archival e-signatures (software signatures) for the following purposes:

— verification of the integrity of metafile and connected sub-records;

— verification of the integrity of the document after structural conversions;

— verification of the authenticity of a partial release of a document when the archive is releasing only a part of the signed and stored patient documentation;

— sealing of a patient record consisting of several parts into a digital envelope and verification of the integrity of the whole record.

The signature shall contain a time stamp. If the national regulations stipulate a developed signature, signing can be realised as a part of the PKI system.

9.6.4 Confidentiality instruments

Requirements for confidentiality are defined in ISO/TS 21547. To meet those requirements a complex set of instruments should be implemented, including

— **Services for identification and authorization of data producers and customers of the archive**: different technologies exist for this purpose, such as PKI services with health professional smart cards, common identity registers, mutual authentication services and identity management services. In many cases the minimum level of trust for identification and authentication of users has been defined by national legislation. The identification services should cover both users and all other entities requiring access to archived data (ISO 15489-1).

— **Privilege management**: the archiving systems should manage privileges of external and internal users. Privilege control should be based on roles (RBAC, ISO 27799). Useful International Standards for this purpose is ISO/TS 22600-1 and ISO/TS 22600-2.

— **Access control services**: if stipulated by national regulations, the eArchive should support context, purpose and consent based access of stored information. Because the eArchive has the responsibility to ensure that legal conditions for access exist before any data disclosure, the access control service should analyse the content of the access request based on rules, restrictions, and on the content of metadata of the record. Necessary information for access can be part of an access request (for example described in the header of HL7 or XML message) sent to the archive.

— **Consent management services**: consent services for record access should analyse received consent information as a part of the access management process. These services have been standardized in ISO/TS 22600-1 and ISO/TS 22600-2.

— **Service managing restrictions for data disclosure**: the metadata of stored objects/records can also include context, purpose and sensitivity-based access restrictions. The access control service should analyse those restrictions as a part of the access management process. Restrictions can also be sent to the archive in the form of separate documents or using the end user negotiation process.

— **Encryption services**: this is one useful technology to ensure that data is not made available during transmission to unauthorized users or processes. Security level required can be defined by national regulation or they can be based on the common agreement between the archive and the customer. In special conditions it is also possible to encrypt data before they are technically stored by the archive.

— **Migration management service**: during the long preservation time of electronic health records one or more data migrations are required. The migration process should be managed in such a way that it fills the security requirements defined in ISO/TS 21547.

9.6.5 Monitoring and accountability instruments

An audit log can be used as a monitoring and accountability instrument. It is also a privacy protection instrument. During the lifetime of the EHR all data capture, record transmission, preservation, records disclosure and destruction events should be logged. All changes to the metadata of the record should also be collected and stored in the log. The integrity and non-repudiation of the audit log can be proven with the help of e-signatures, archival time stamps and e-notary services.

The preservation time of the audit log information should meet national regulations.

If national legislation allows patients or citizens to electronically access their own audit logs to know who has used their health information, when and for what purpose, the eArchive should maintain this kind of service.

9.6.6 Non-repudiation instruments

A non-repudiation service is an instrument that can be used to:

— verify the existence, contents and status of a record, object or document at a certain time;

— prove the time and content of events during the preservation time;

— prove the content of audit logs.

PKI services, archival time stamps, event records, read only memories, log files and electronic notary services are tools that can be used to build non-repudiation services.

9.6.7 Instruments for secure communication

A number of security and privacy protection risks exist in relation to the communication between the EHR system and the eArchive concerning integrity, confidentiality, denial of service and authenticity. The most common threats are

— modification of the content of the record;

— loss of information;

— eavesdropping;

— theft of the data;

— data replication attacks;

— virus and worm propagation;

— impersonating a legitimate user;

— isolating servers by DNS attacks.

Instruments for secure communication between the eArchive and customers/data providers include

— encryption of the information sent to the eArchive;

— electronically sealed envelopes;

— certificates;

— authentication of the communicating server;

— firewalls;

— virtual private network services (VPN);

— anti-virus checking tools.

Selection of security services and tools for EHR communication between the EHR system, eArchive and customers should be based on results of the risk analysis and the process described in Clauses 8 and 9. Depending on the architecture of the eArchive, communication can occur inside the LAN of the health service provider or via external communication services. The Internet can also be used as a communication channel, as can the mobile communication network.

9.7 Administrative instruments

An archiving organization should specify authorities and their responsibilities regarding the archiving process and the responsibility of record management. Those are likely to be the following, based on the definition given in ISO/TR 15489-2:

— establishment of the archival authority and its responsibilities;

— a senior security manager should be assigned to the highest level of responsibility for security management;

— records management professionals of the archiving organization have primary responsibility to implement security controls and instruments;

— negotiation and contracts;

— monitoring and auditing;

— certification.

9.8 Metadata

9.8.1 Introduction

Metadata is information describing the context, content and structure of records and their management through time (ISO 23081-1). Metadata enables the creation of archival packet, registration of EHRs, long-term availability and usability of the EHR, access and disclosure, preservation, and disposition of records. Metadata ensures the reliability, usability and integrity of archived health information. Metadata is one of the security instruments used for trusted long-term preservation of health records.

During the eArchiving process metadata is initially added by the EHR system to information captured for archiving purposes. The eArchive adds archival metadata to the record for preservation management purposes.

From a privacy protection point of view, it is good practice not to include personal information in the metadata of the EHR. Because metadata is in many cases used for retrieval purposes, it can include such detailed information as patient identification and service provider's name. If the metadata includes personal information, the same security and privacy protection rules applying to the EHR should be used for its metadata.

9.8.2 EHR metadata

Archives should preserve not only data but also information (ISO/TS 21547, Requirement 1). The data received by the archive should contain all necessary retention and security meta-information to support long term archiving. This metadata includes the following parts:

— descriptive metadata;

— content information metadata;

— administrative metadata;

— source metadata;

— digital provenance metadata (information about changes the file has undergone since its birth);

— rights metadata (e.g. conditions and restrictions for legal access);

— security metadata (e.g. context, purpose, sensitivity, access restrictions and obligations).

The health record itself has a contextual structure. Standards such as EN 13606, openEHR, HL7 CDA and DICOM have defined models for the structure of the EHR (e.g. openEHR defines folders, compositions, headed sections, clusters and data values and HL7 CDA uses a document model comprised of header and body with section structure).

Data values used in the EHR can be represented in different kinds of data types such as

— narrative text;

— coded terms;

— quantities and numeric data;

— references and links (for example to other patient folders and knowledge bases);

— bit streams/maps (e.g. digital images, ECG and EEG signals);

— a variety of multimedia file formats.

For long-term availability, the metadata of an EHR should include information describing the data types used.

For security purposes each EHR (and if necessary all its objects) should have a unique identifier. One possible global identifier is the ISO/IEC 9834-3 UID International Standard. In addition, it should be considered whether the URN identifier might be used instead of the UID number, in accordance with IETF/RFC 2141. The metafile of the record/object should include the unique identifier.

ISO 23081-1 is a metadata International Standard that is aimed for use within the frameworks of the various parts of ISO 15489-1. ISO 23081-1 defines the following metadata components to support ISO 15489-1:

— metadata about the record itself;

— metadata about business rules or policies and mandates;

— metadata about agents;

— metadata about processes;

— metadata about records management processes.

Another candidate metadata International Standard is METS (metadata encoding and transmission standard) and MIX (metadata for images in XML Standard). METS consists of the following parts:

— descriptive metadata;

— structural map (orders objects into a browseable hierarchy);

— content file section;

— administrative metadata;

— technical metadata;

— source metadata;

— digital provenance metadata (the changes a file has undergone since its birth);

— rights metadata (conditions of legal access).

Another available metadata standard is Dublin Core.

EN 13606 also defines a data extraction model with security meta-information.

Security metadata for long-term preservation of EHRs should be selected as a part of the process described in Clause 8.

9.8.3 Archival metadata

The eArchive should define necessary metadata and the elements it needs for long-term preservation purposes inside the archiving organization (ISO 14721).

The archival metadata includes the following information:

— archive administrative data;

— security information;

— customer profile;

— preservation process history;

— request tracking information;

— preservation policy information;

— packing information.

The eArchive should select adequate metadata based on the archiving policy and risk analysis. It should also select the metadata standards it employs.