SLOVENSKI STANDARD
SIST ENV 12924:2003

01-oktober-2003

Medicinska informatika ï Kategorizacija varnosti in zaġļ ite v informacijskih sistemih zdravstvenega varstva

Medical Informatics - Security Categorisation and Protection for Healthcare Information Systems

Medizinische Informatik - Sicherheitskategorisierung und Schutz für Informationssysteme im Gesundheitswesen

Informatique de santé - Catégorisation et protection des systemes d'informations de santé

Ta slovenski standard je istoveten z: **ENV 12924:1997**

ICS:

35.240.80	Uporabniške rešitve IT v zdravstveni tehniki	IT applications in health care technology

SIST ENV 12924:2003 **en**

EUROPEAN PRESTANDARD
PRÉNORME EUROPÉENNE
EUROPÄISCHE VORNORM

ENV 12924

November 1997

ICS 11.020; 35.240.70

Descriptors: medicine, data processing, information interchange, safety, protection of information

English version

Medical Informatics - Security Categorisation and Protection for Healthcare Information Systems

Informatique de santé - Catégorisation et protection des systèmes d'informations de santé

Medizinische Informatik - Sicherheitskategorisierung und Schutz für Informationssysteme im Gesundheitswesen

This European Prestandard (ENV) was approved by CEN on 1 November 1997 as a prospective standard for provisional application.

The period of validity of this ENV is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the ENV can be converted into a European Standard.

CEN members are required to announce the existence of this ENV in the same way as for an EN and to make the ENV available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the ENV) until the final decision about the possible conversion of the ENV into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Central Secretariat: rue de Stassart, 36 B-1050 Brussels

Ref. No. ENV 12924:1997 E

Contents

Foreword

This European Prestandard has been prepared by Technical Committee CEN/TC 251 "Medical informatics", the secretariat of which is held by IBN.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this European Prestandard: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

Introduction

Information systems of healthcare establishments throughout Europe have been providing essential administrative support for both clerical and management functions for many years. In recent years this support has extended to include the provision of information in a clinical context, not only within a hospital, but across networks involving both primary and secondary healthcare in a number of different countries. These projects have enabled clinicians to store information in a more structured manner and to re-present it in a more helpful format to the right people when it is needed - wherever they may be located.

These advances in information management have themselves introduced new threats to the status of that information and the need for measures to ensure the confidentiality and the integrity of the information has never been greater. In addition, as these opportunities are realised and the telematics processes become a routine part of working practices, the need to ensure the continued availability of the right data in the right place at the right time will become even more vital; for many healthcare establishments it already is an extremely important factor. These three requirements of telematics - availability, confidentiality and integrity - are now collectively considered to be in the domain of security.

Information systems which process administrative data and do not directly influence patient care are sometimes excluded from considerations of security. They cannot be regarded as safety related but experience has shown that breaches of security of administrative systems often do have a consequential effect on patient care, if only in that they divert attention and resources from patient care issues. For this reason healthcare administrative systems are included within the scope of this standard.

In order to determine how best to protect telematic systems from any of the vast array of events which may threaten to compromise security, it is first advisable to consider the specific nature of the risks to which a particular system is exposed. For anything other than a very small healthcare establishment such an exercise is usually time-consuming and requires particular skilled resources. In an environment, such as healthcare, where competition for scarce resources is especially demanding, many organisations have found it difficult to justify the expense of conducting a risk analysis exercise.

Work in this area has been proceeding in a number of European countries for some years. This has shown that there is a large degree of uniformity of security related risks among healthcare establishments of all kinds. This stems mainly from the fact that the most important influences on the protection required is the type of data which a system processes and the use which is made of the resulting information output to the end user. There are, of course, other influences which will affect the way in which security mechanisms will be implemented but experience has shown that the common target of patient well-being permits the specification of a standard set of security requirements and recommendations which will be relevant across all healthcare establishments.

It should be realised that, however well an information system is protected, total security in the sense that a breach could never occur, is not achievable. The best that can be done is to reduce the risk of the occurrence of a security breach to a level which is operationally acceptable to the management of a healthcare establishment. The protection specified in this European Prestandard has been set to a level which current experience suggests represents good management practice within European healthcare establishments. This experience has been gained from specific risk analysis exercises in various healthcare establishments throughout Europe.

The Security categorisation model and guidance on how to use the model is defined in clauses 5-7 with informative annexes A and B.

1 Scope

This European Prestandard specifies a model and a method of categorising automated healthcare information systems in the context of security and privacy. Security has been taken to mean the preservation, to an acceptable level, of data availability, confidentiality, and integrity. For each system category specified a corresponding set of protection requirements and recommendations is provided which is appropriate to the level of risks inherent in that category.

This European Prestandard applies to all automated information systems which process healthcare data. This includes systems which contribute directly to patient care, for example reports of laboratory test results; but it also includes statistical systems as well as administrative systems which provide operational support for the healthcare establishment itself, for example staff payroll, personnel, planning and financial support systems. However, systems where confidentiality is considered to be unimportant i.e. the information is in the public domain, are not covered by this European Prestandard. The target audiences for this European Prestandard are the consumers/procurers of secure information systems in healthcare and developers/manufacturers of secure information systems in or for healthcare.

Implementation of the terms of this European Prestandard is regarded as a responsible management response to the obligations of national and European laws as well as the expectations of the public for a high standard of security of healthcare information.

2 Normative references

This European Prestandard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter.

For dated references, subsequent amendments to or revisions of any one of these publications apply to this standard only when incorporated in it by amendment or revision.

For undated references the latest edition of the publication applies.

PrENV 12251	Medical Informatics Secure User Identification for Healthcare: Management and Security of Passwords - Healthcare Oriented IT Security Functionality Class. Draft FFV.
ISO 7498-2:1989	Information Processing Systems - Open Systems Interconnection -Basic Reference Model - Part 2: Security Architecture
ISO/IEC 9594-8:1990	Information technology - Open Systems interconnection : The Directory - Part 8: Authentication framework.
ITSEC	Information Technology Security Evaluation Criteria. Version 1.2, 1992.
Common Criteria	Common Criteria for Information Technology Security Evaluation, CCEB-96/011, Version 1.0, 31/01/1996.

3 Definitions

For the purposes of this European Prestandard the following definitions apply

access control: The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner. [ISO 7498 - 2]

accountability: The property that ensures that the actions of an entity can be traced. [ISO 7498 - 2]

audit trail: Data collected and potentially used to facilitate a security audit. [ISO 7498-2]

authentication: The corroboration that an entity is the one claimed. [ISO 7498 - 2]

authentication token: A device allocated to an entity to assist the authentication of that entity.

authorisation: The granting of rights, which includes the granting of access based on access rights. [ISO 7498 - 2]

availability: The property of being accessible and useable upon demand by an authorised entity. [ISO 7498 - 2]

confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes. [ISO 7498 - 2]

countermeasure: A measure designed to prevent a security breach, limit its impact or detect its occurrence.

criticality: The degree of importance assigned to information denoting its need for protection against integrity and availability security breaches.

denial of service: The prevention of authorised access to resources or the delaying of time-critical operations. [ISO 7498 - 2]

digital signature: Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the unit and protect against forgery e.g. by the recipient. [ISO 7498 - 2]

encryption: The cryptographic transformation of data to produce ciphertext. [ISO 7498-2]

health care data: Data which are input, stored, processed or output by the automated information system which support the business functions of the Health care Establishment. These data may relate to person identifiable records or may be part of an administrative system where persons are not identified.

impact: The embarrassment, harm, financial loss, legal or other damage which could occur in consequence to a particular security breach.

integrity: The property that data has not been altered or destroyed in an unauthorised manner. [ISO 7498 - 2]

password: Confidential authentication information composed of a string of characters. [ISO 7498 - 2]

protection profile: A reusable and complete combination of security objectives, functional and assurance requirements with associated rationale. [Common Criteria]

recovery: The restoration of an information system back to an error-free and secure state from which normal operation can resume.

risk: The aggregate effect of the likelihood of occurrence of a particular threat with the degree of vulnerability to that threat and the potential consequences of the impact to the organisation if the threat did occur.

security: The combination of availability, confidentiality and integrity. [ITSEC]

security audit: An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policies and operational procedures, to detect security breaches and to recommend any indicated changes in control policy and procedures. [ISO 7498 - 2]

security breach: The unauthorised disclosure, destruction, modification or withholding of information.

security objective: A statement of intent to counter a given threat or enforce a given organisational security policy. [Common criteria]

security policy: A statement of the set of rules, measures and procedures that determine the physical, procedural and personnel security controls imposed on the management, distribution and protection of assets.

security target: The statement of security requirements and functional specifications to be used as baseline for an evaluation. [ITSEC]

sensitivity: The degree of importance assigned to information denoting its need for protection against confidentiality related security breaches.

strong authentication: Authentication by means of cryptographically derived credentials. [ISO/IEC 9594- 8]

threat: An action or event that might prejudice security. [ITSEC]

top level security objective: A generalised statement of intended security goals relating to the availability, confidentiality and integrity of health care information.

vulnerability: A security weakness due to failures in analysis, design, implementation or operation. [ITSEC]

4 Abbreviations

The following abbreviations are used for the terms in this European Prestandard:

ACI	Availability, confidentiality and integrity
HCE	Healthcare establishment
HCIS	Healthcare information systems
IT	Information technology
LAN	Local area network
LCA	Logical connectivity assumptions
PC	Personal computer
PCA	Physical connectivity assumptions
PEA	Physical environment assumption
PP	Protection profile
SU	Small user
TLSO	Top level security objectives

5 Security categorisation model

The objective of a security exercise is to make a healthcare information system (HCIS) (be it abstract, designed or real) secure. The usual process for achieving this objective is graphically shown in Fig. 1.

All security requirements and recommendations derive from the security environment and expert analysis of the security problems in the context of the environment. That analysis leads to a statement of risks which is used as the foundation for development of requirements and recommendations.

If relevant to the user organisation, a parallel activity may be, or may already have been, undertaken to develop relevant security policies. Such security policies may be pertinent to security in general or may be IT specific technically oriented policies.

The process of building policies develops the top level security objectives (TLSOs) based on the stated risks using knowledge about the environment and incorporating any required policy constraints. The process is essentially an expert judgement. In this pre-standard, healthcare systems are categorised in six categories, based on the nature of the data they process and their environment. Thus, TLSOs lead to pre-defined system categories.

The process of developing requirements refines the TLSOs into a more detailed statement of information systems security requirements and recommendations and is subject to environmental constraints. The process is essentially one of requirements capture and analysis. Requirements capture may be specific to a known HCIS leading to a security requirements statement for that HCIS, or it may be directed towards determining security requirements for solving a more general class of problems. In the latter case, the requirements may be expressed as a Protection Profile (PP).

A PP is in this European Prestandard a unique set of security objectives, requirements and recommendations for a particular class of HCISs which are intended to meet a common need for HCIS security. Users can use a PP to express their requirements in an abstract manner. The contents of a PP are depicted in Fig. 2. Their descriptions are given below.

5.1 System categories

System categorisation is primarily made with respect to the information associated with the HCIS in question. It describes the nature of the information that it stores, processes or communicates according to the values of the availability, confidentiality and integrity (ACI) attributes (cf. Clause 6.1).

In addition to this basic categorisation, environmental assumptions regarding the system may be applicable (cf. Clause 6.4).

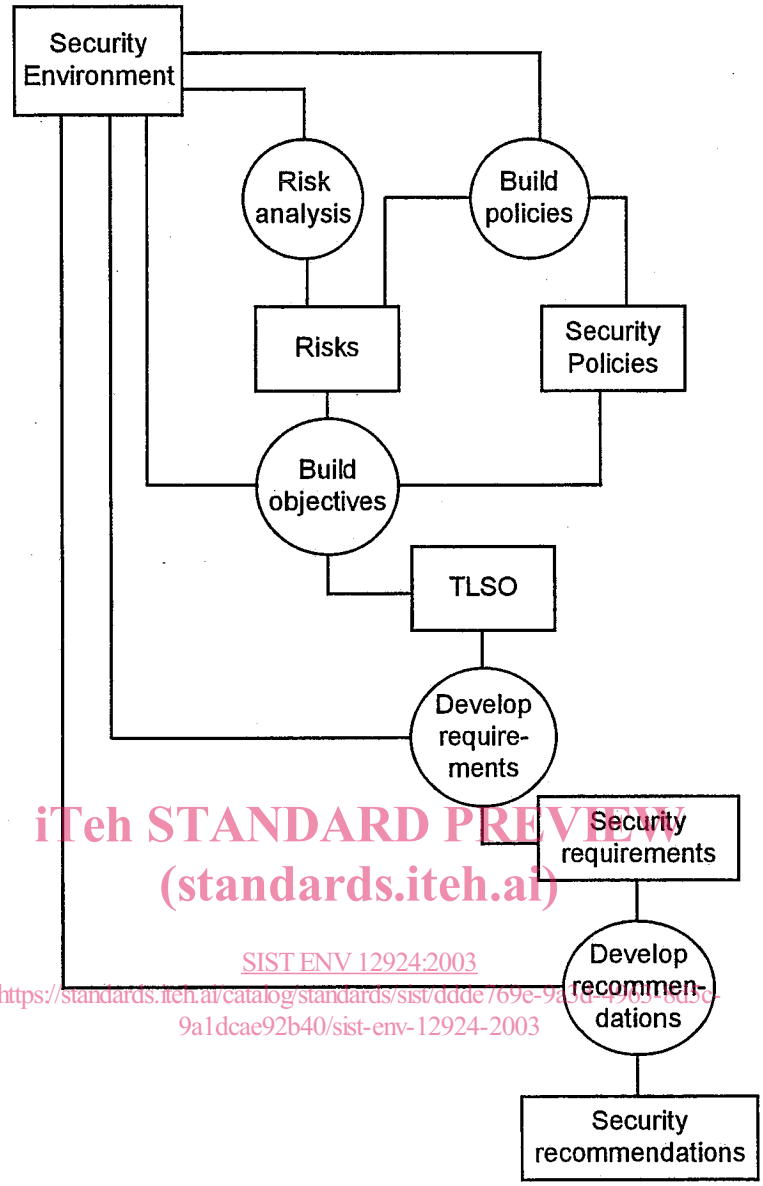

Figure 5.1 Derivation of requirements and recommendations

5.2 Requirements

The requirements clauses provide the security functional requirements for the HCIS. Security functional requirements are provided as groups and as components. Groups of functional requirements comprise functional requirements aimed at meeting the same security objective.

Each of the requirements clauses is broken down into three component parts.

Baseline requirements. These are the requirements that every HCIS which handles anything other than non sensitive data shall meet.

Additional requirements. These are the requirements that shall be met, in addition to the baseline requirements, by all HCISs handle personal identifiable data.

Environment dependant requirements. These requirements shall be met by all HCISs with certain user and environmental characteristics, in addition to the baseline and the additional requirements.

At all levels recommendations are given on certain choices, preferences or specifics in relation to the requirements given.

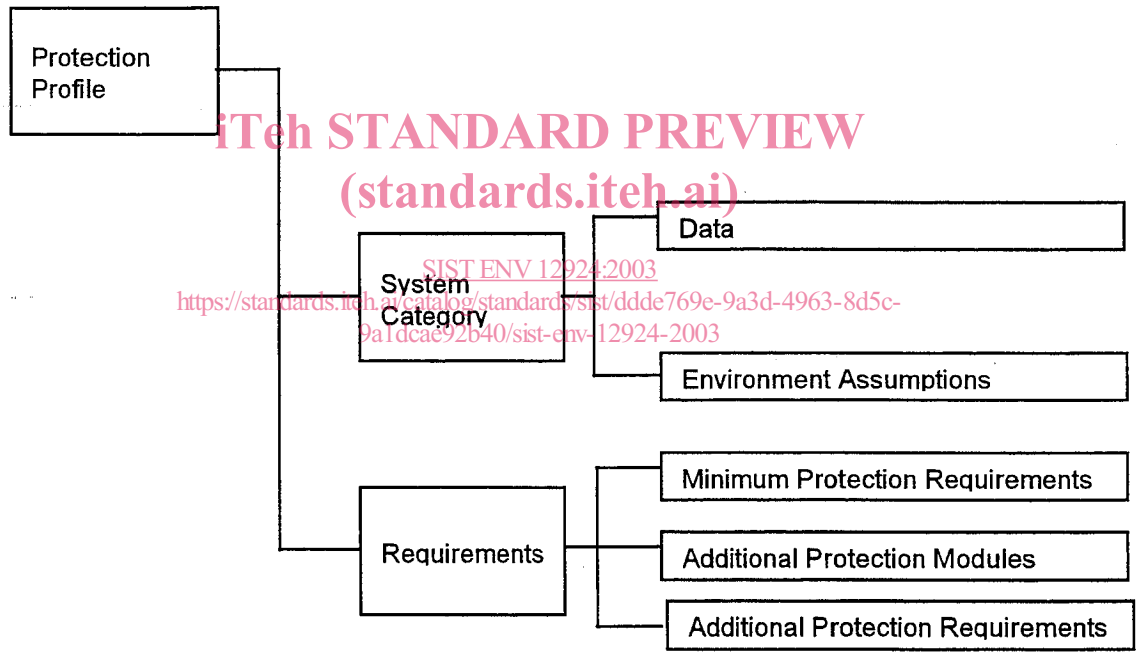

Figure 5.2 Contents of a Protection Profile

5.3 Healthcare information systems characteristics

The major characteristics of a HCIS, in the context of security, are:

Data input, stored, processed, and output.

Hardware & software configuration.

People in many different possible roles, including designers and/or suppliers, technical support staff, users and even visitors.

The overall environment where the configuration is cited, the data used and where people attend and/or set up communication.

Usage, including procedures of system use.

Different implementations of one or more of these system characteristics can lead to different requirements for protection. Such differences may involve security functions, products or issues of strength of protection (referred to as "protection levels").

5.3.1 Data

The most significant contribution to the requirement for security is provided by the types of data used within the system. This factor dominates all others as far as the health care requirement is concerned. This is because of the very strong need to preserve the confidentiality, integrity and availability of all types of data within health-care systems, but especially those related to patients.

It is necessary to separate out the need for confidentiality from that for integrity and availability.

The implications of disclosure of data are determined solely by the nature of the information conveyed by the data, whereas the implications of corrupt or absent data are determined not only by the type of data but also by the use which is to be made of them.

5.3.2 Hardware & software configuration

Most of the elements of a system configuration contribute very little to the security requirement in itself.

Indeed, a specific operating system or data base management system will not affect the security requirement. It may be that the required protection feature is not provided, but it will not be the software itself which gives rise to the requirement.

5.3.3 People

One of the major characteristics of healthcare information systems, which sets the security requirements apart from other governmental or commercial systems, is that unauthorised people often cannot be distanced from the system assets. This, coupled with the fact, that healthcare organisations collectively comprise the biggest employer in the world, exposes HCIS to a very large population which could potentially harm the system through either accidental or deliberate actions.

The characteristics of this population will, in general, be fairly consistent in that they provide a very broad range of causes for most accidents as well as a variety of motivation for deliberate harm which might happen to any one system. From a security viewpoint, the main consideration, will be centred on the differences which arise from the different opportunities available for people to gain access to the system.

For wards and other areas open to the public, the vulnerabilities are known and will again be at a consistent level across all HCEs of similar type. The differences will involve possible access to the central computing resources, either physically or logically.

Opportunity for physical access will be a function of the operational environment and is discussed below.

Logical access opportunity will be provided remotely by networking features. This is also part of the HCIS environment and is discussed below.

Thus, the "people" problem makes no direct contribution to system categorisation, as its influence is consistent across all HCIS. However, the different vulnerabilities which people may exploit will be captured through consideration of other system characteristics viz. environmental.

5.3.4 Environment

Two aspects of an HCIS environment play a major role in the security requirement of the system:

Asset distribution

System connectivity

All HCEs will contain a room which might be termed a "computer room". At its very simplest, this could mean that the room contains a PC and a printer, and perhaps a modem and a telephone line. It could, of course, contain a number of servers, peripheral devices, and communications equipment or a mainframe computer and its associated equipment. In many HCEs, in addition to the computer room, there will be other offices and reception points housing system assets, such as terminals, routers, etc. Finally, in some HCEs and certainly in hospitals, system assets will be located in wards and sometimes even in corridors.

The main environmental aspect which merits special attention is that of system connectivity. If the system under consideration is networked and that network is connected to others under different organisational controls, the security requirements will tend to be stronger (or at least different) than for a stand-alone system.