SLOVENSKI STANDARD
SIST-TP CR 13694:2003

01-oktober-2003

Zdravstvena informatika – Standardi kakovosti glede varnosti in zaščitenosti programske opreme v zdravstvenem varstvu

Health Informatics - Safety and Security Related Software Quality Standards for Healthcare (SSQS)

Ta slovenski standard je istoveten z: CR 13694:1999

ICS:

03.120.99	Drugi standardi v zvezi s kakovostjo	Other standards related to quality
35.240.80	Uporabniške rešitve IT v zdravstveni tehniki	IT applications in health care technology

SIST-TP CR 13694:2003 **en**

CEN REPORT

RAPPORT CEN

CEN BERICHT

CR 13694

August 1999

ICS

English version

Health Informatics - Safety and Security Related Software Quality Standards for Healthcare (SSQS)

This CEN Report was approved by CEN on 16 June 1999. It has been drawn up by the Technical Committee CEN/TC 251.

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. CR 13694:1999 E

CONTENTS

A3 American Society for Testing and Materials (ASTM) (USA)
A4 Computer-based Patient Record Institute (CPRI) (USA)
A5 HL7 Inc (Canada)
A6 Privacy Commissioner (New Zealand)
A7 Standards Australia (SA) (Australia)
A8 Standards Australia/Standards New Zealand

ANNEX B: Non-Healthcare and Security Related Standards

B1 British Standards Institution (BSI) (UK)
B2 ITSEC (UK)
B3 Central Computer and Telecommunications Agency (CCTA) (UK)
B4 Accredited Standards Committee (ASC) X12. (USA)
B5 ISO/IEC (International)

ANNEX C: Healthcare and Safety Related Standards

C1 CEN TC/251 (Euro)
C2 Medical Devices Agency (UK)
C3 British Standards Institution (UK)
C4 IEC (International)
C5 IEEE (USA)
C6 American Society for Testing and Materials (ASTM) (USA)

ANNEX D: Non-Healthcare and Security Related Standards

D1 IEC (International)
D2 Ministry of Defence (UK)
D3 Requirements and Technical Concepts for Aviation (RTCA) Inc. (USA)

ANNEX E: Standards in Quality Management and Quality Assurance

ANNEX F: Projects Related to the Security of HISs

F1 SEMRIC
F2 MEDSEC
F3 SEISMED
F4 ISHTAR
F5 G7 ENABLE
F6 TEAC – HEALTH

FOREWORD

This CEN Report has been prepared under the direction of the European Committee for Standardization (CEN). The preparation of this CEN Report was undertaken by PT 38 under the direction of Working Group III of CEN/TC 251 under Work Item: SSQS.

This CEN Report has undergone a review under the CEN Request for Comments Procedure and subsequently approved by WGIII during the WGIII meeting held in London, UK on 1999-02-01/02.

TC 251 is requested to approve this CEN Report as the final deliverable fo PT38.

An electronic copy of this CEN Report is available from the CEN/TC 251/WGIII website on;

http://forum.afnor.fr/WORK/AFNOR/GPN2/S95I/PRIVATE/WEB/ENGLISH

INTRODUCTION

Healthcare Information Systems (HISs) are increasingly being used within the healthcare sector, and, as a consequence, they are coming closer to the patient and clinicians are becoming much more dependent on their use. For instance, these systems can range from simple databases that are used to record and store medical data, to medical expert systems that are used to assist in the process of diagnosis of an illness. Hence, any malfunction of HISs can have implications for patient safety. Also, unauthorised access to medical data can lead to a breach in patient confidentiality or more seriously unauthorised changes to medical data can lead to incorrect diagnosis which can have an impact on patient safety.

Due to the nature of HISs and the environment in which they must operate, these systems must be developed to ensure that the issues of safety and security are pursued to a level that is considered to be acceptable for the application. Thus, there is a need for standards and documents which ensure that;

- HISs are developed using appropriate techniques;
- HISs are certified to be safe and secure;
- HISs are used in the appropriate manner;
- HISs are adequately maintained;
- incidents concerning HISs are monitored.

1. SCOPE

This CR presents a review of the existing and emerging standards that are, or may be, applicable to HISs. The type of standards that are considered are those that focus on the issues of software safety, security, confidentiality, and integrity. This CR also provides a discussion of the issues that need to be addressed in compiling a guidance for purchasers and developers of HISs.

This CR also examines some standards which do not necessarily concern HISs but instead refer to general computer-based systems. These standards are examined because it is considered that they may be applicable, or adapted, to Healthcare Systems. The standardising organisations examined in this review include: IEC, CEN, BSI, ASC X12, ASTM, CPRI and IEEE.

The discussion in this CR highlights that many standards and guidelines have been developed to address the security of HISs, but few standards address the safety issues. However, several safety standards do exist that address medical devices, medical equipment or general safety related systems. These standards may be adapted or used to develop safety standards for HISs.

From the review presented in this CR, it is concluded that future standardization work in HISs should give greater consideration to the safety aspects of these systems. Specifically, the areas that should be addressed are: determining the criticality of HISs, defining the approaches and methods for developing HISs, providing facilities for performing clinical testing of HIS and the setting of an incident reporting mechanisms to monitor the in-service operation of HISs.

2. REFERENCES

This CR cites the following key references at appropriate places in the text. A fuller description of reference documents and projects is provided in the appendices;

BS 7799 (Part 1)	Information Security Management – Code of Practice
BS 7799 (Part 2)	Information Security Management – Accreditation Process
EN 1441	Medical Devices – Risk Analysis.
EN 60601-1-4	Medical Electrical Equipment – Part 1: General Requirements for Safety – 4. Collateral Standard: Programmable Electrical Medical Systems.
ENV 12924	Medical Informatics – Security Categorisation and Protection for Healthcare Information.
IEC 61508	Functional Safety – Safety Related Systems.
ITSEC	Information Technology Security Evaluation Criteria.

[1] I. Peterson, "Fatal Defects", Vintage Books, ISBN 0-0991-9742-1, 1996.

[2] P.G. Neumann, "Computer Related Risks", Addison Wesley, ISBN: 0-201-55805-x, 1995.

[3] J.C. Laprie, 'Dependability: A unifying concept for reliable computing and fault tolerances', In T. Anderson (Ed.), 'Dependability of Resilient Computers' Blackwell Sciences Publications, Oxford, 1989, pp 1-28.

[4] J.A. McDermid, 'On dependability, its measurement and its management', High Integrity Systems, Vol. 1, No. 1, 1994, pp 17 -26.

[5] R.J. Anderson, "Safety and Privacy in Clinical Information Systems",

[6] J. Vowler, "Patient care at risk from millennium bug", Computer Weekly, May 1997, p. 3.

[7] R.S. Pressman, "Software Engineering: a practitioner's approach", McGraw-Hill International, 1994.

[8] C. Mazza, J. Fairclough, B. Melton, D. De Pablo, A. Scheffer, and R. Stevens, "Software Engineering Standards", Prentice Hall, 1994.

3. DEFINITIONS

Accountability:	the property that ensures that the actions of an entity can be traced [ISO 7498-2]
Authentication :	the provision of assurance of the claimed identity of an entity (ISO/IEC 10181-2: 1996]
Availability:	the prevention of the unauthorised withholding of information or resources [ITSEC]
Confidentiality:	the prevention of the unauthorised disclosure of information [ITSEC].
Dependability:	the property of a system in which reliance can justifiably be placed on the service that it delivers [3], [4].
Integrity:	the prevention of the unauthorised modification of information [ITSEC].
Safety:	the freedom from unacceptable risk of harm (or damage) that may be done to human life (or an environment) by a system. [IEC 61508]. This is further defined in Section 5.1.1.
Security:	the preservation of the confidentiality and integrity of data as well as ensuring the accountability and availability of data. [ENV 12924]. This is further defined in Section 5.1.2.
Quality:	the totallity of features and characteristics of a product, process or service that bear on its ability to satisfy its stated or intended needs

4. ACRONYMS

ALARP – As Low As is Reasonably Practicable.
AIM - Advanced Informatics in Medicine.
ASC - Accredited Standards Committee.
ASTM - American Society for Testing and Materials.
BSI - British Standards Institution.
Can. - Canada.
CCTA - Central Computer and Telecommunications Agency.
CEN - Comite European de Normalisation.
CORBA - Common Object Request Broker Architecture.
CPRI - Computer-based Patient Record Institute.
CPRS - Computer-based Patient Record System.
CRAMM - CCTA Risk Analysis and Management Methodology.
CR - CEN Report.
D - Germany.
DC - Draft Copy.
DERA - Defence Evaluation & Research Agency.
DHE - Distributed Healthcare Environment.
EEC - European Economic Community.
EDIFACT - Electronic Data Interchange For Administration, Commerce and Transport.
ENV - European Pre-standard.
EWICS - European Workshop on Industrial Computer Systems.
Euro - European
FM-HSP/FR - Framework for Formal Modelling of Healthcare Security Policies.
GISA - German Information Security Agency.
HC - Health Care.
HDLC - High Level Data Link Control.
HIS – Healthcare Information System.
HL7 - Health Level 7.
I - Issued.
IEC - International Electrotechnical Commission.
IEEE - Institute of Electrical and Electronic Engineers.
ICD - Intermittently Connected Devices.
ICT - Information and Communications Technologies.
ISHTAR - Implementing Secure Health Telematics Application in Europe
ISIS - Information Society Initiatives in Standardization.
ISO - International Organisation for Standards.
IT - Information Technology.
ITSEC - Information Technology Security Evaluation Criteria.
ITSEM - Information Technology Security Evaluation Manual.
MEDSEC - Health Care Security and Privacy in the Information Society.
N - No.
NHS - National Health Service.
NHS IM&T - National Health Service Information Management and Technology.
NR - Not Ready.
NZ - New Zealand.
OII - EC Open Information Interchange.
PES - Programmable Electronic System.

prENV - A European Pre-standard.
PT - Project Team.
RICHE - Reseau d'Information et de Communication Hospitalier Europeen.
RTCA - Requirements and Technical Concepts for Aviation.
SA - Standards Australia.
SAFE-ID - Safety Procedures for Identification of Patients and Related Objects.
SEC-COM - Security for Healthcare Communication.
SEC-COM/FR - Framework for Security Protection of Healthcare Communication.
SEC-ICD - Security Requirements for Intermittently Connected Devices.
SECREQ-ICD/FR - Framework for Security Requirements for Intermittently Connected Devices
SEC-ID/CARDS - Secure User Identification for Healthcare Strong Authentication using Microprocessor Cards.
SRS - Safety Related Systems.
SNZ - Standards New Zealand.
Saf. - Safety.
SDO - Standards Developing Organisation.
Sec. - Security.
SEISMED - Secure Environment for Information Systems in Medicine.
SEMRIC - Secure Medical Record Information Communication.
SIREN - Security in Regional Networks.
STEP - Standards Enforcement in Procurement Process.
TC - Technical Committee.
THIS - Trusted Health Information Systems.
TR - Technical Report.
UHID - Universal Healthcare Identifier.
UK - United Kingdom.
USA - United States of America.
WG - Working Group.
Y - Yes.

5. CLARIFICATION OF ISSUES IN HIS's

Due to the increasing use of computer-based systems within the Healthcare sector, information systems are becoming more intimately involved in patient care and Healthcare professionals are becoming more dependant upon their use. For example, information systems are being used to assist in the diagnosis and treatment of patients and to form centralised and distributed databases of patient medical records.

Although, currently, HISs generally only form part of an overall process, any malfunction or vulnerability of these systems can be a threat to patients. Such incidents can result in damage to the health of patients, claims for legal compensation or penalties, and loss of public confidence. This is exemplified by systems used in areas such as drug prescription, radiation treatment, the design of linear accelerator software, and the control of ambulance services [1], [2]. Therefore, while the importance of integrity in HISs is recognised, it is usually the overall system that causes harm rather than the software within the system. Standards that evaluate the whole system involving the software help to reduce risks to patients and to give confidence to purchasers.

This CR reviews standards addressing the complete life cycle of a HIS. It considers the pre-purchasing needs of a customer; the requirements that should be met by a supplier; the maintenance and servicing of systems; and incident reporting mechanisms.

When reviewing the standards regarding HISs, the following issues need to be clarified:

5.1 DEFINITIONS OF SAFETY, SECURITY AND DEPENDABILITY

5.1.1. Safety

The notion of safety is usually associated with the prevention of the harm (or damage) that may be done to human life (or an environment) by a system. In the context of safety standards for computer-based systems [IEC 61508; EN 1441; EN 60601-1-4; Medical Devices Directive 93/42/EEC], safety is defined as the freedom from unacceptable risk of harm. In this definition, the terms harm and risk have particular interpretations, and these are:

(i) harm is the physical injury, or the damage to health or property, that may be caused by the system;

(ii) risk is the probable rate of occurrence of a hazard causing harm and the degree of severity of the harm. Thus, the concept of risk has two elements:
   (a) the frequency with which a hazard occurs, and
   (b) the consequences of the hazardous event.

   A hazard is understood to be a situation in which there is a potential for human injury.

Thus, the concept of risk forms an integral part of the notion of safety.

The implications of the failure of a safety-related system can vary greatly between applications, and this leads to concepts such as the "level of safety" and the "safety integrity" of a system. IEC 61508 describes these terms as follows:

(i) the level of safety of a system is defined as a level of how far safety should be pursued in a given context, assessed to an acceptable level of risk, based on the values of society. In order to achieve an acceptable level of risk, it needs to determined whether:

(a) the risk is so great that it must be refused altogether; or
(b) the risk is, or has been made, so small as to be insignificant, or
(c) the risk falls between (a) and (b), and that it has been reduced to the lowest level practicable (bearing in mind the benefits flowing from its acceptance and taking into account the costs of any further reduction).

With respect to (c) the ALARP principle requires that any risk must be reduced as far as is reasonably practicable or to a level which is "as low as reasonably practicable". If a risk falls between the two extremes (i.e. the unacceptable region (a) and the broadly acceptable region (c)) and the ALARP principle has been applied, then the resulting risk is the tolerable risk for that specific application;

(ii) safety integrity denotes the probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a period of time. This definition focuses on the reliability of the safety-related system to perform the safety functions. In determining safety integrity, all causes of failure (both random hardware failures and systematic failures) which lead to an unsafe state must be considered. Some types of failures may be quantified whereas others can depend on factors that cannot be quantified but considered qualitatively. The IEC 61508 defines four types of discrete safety integrity levels, and these specify the safety integrity requirements of the safety functions to be allocated to the safety-related system.

5.1.2 Security

The term security, when applied to information systems, is commonly understood to mean the protection of a system's assets such as the information and information processing resources. Specifically, security has been defined [ITSEC, ENV 12924, MEDSEC, BS 7799] as the preservation of the confidentiality and integrity of data as well as ensuring the accountability and availability of data. These terms have the follows interpretation:

(i) *confidentiality* ensures that information is not made available or disclosed to unauthorized individuals, entities or processes. Thus, the protection of personal medical data is a vital component of medical treatment; in some cases the anonymity of a patient may need to be preserved;

(ii) *integrity* denotes that the data has not been altered or destroyed in an unauthorized manner. The subtlety associated with this notion is that unauthorized actions are not only restricted to unauthorized persons but may be performed by authorized users. This situation introduces further difficulties in the health care domain, where professionals are personally responsible and mostly liable for their decisions in favour of a particular action or against it;

(iii) *accountability* is concerned with ensuring the actions performed by an entity on a system can be traced uniquely to that entity. This property can be supported by mechanisms such as authentication and non-repudiation of an entity, as well as maintaining audit logs. Authentication is concerned with the verification of the identity of a user, and non-repudiation provide the assurance that a seemingly authentic but possibly forged message cannot subsequently be claimed to be a forgery;

(iv) *availability* is concerned with ensuring that data is accessible and useable upon demand by an authorized entity.

Although the notions of confidentiality, integrity, accountability, and availability have been presented separately, they are related. For instance, mechanisms must be implemented in a system that make it possible to provide the correct service to authorised, or trusted, users.

To ensure that a system's assets are adequately protected, and to provide a level of assurance in the operation of a system, risk analysis must be performed. In the context of security, a risk is defined as 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. A threat is defined as an action or event that might prejudice the security of a system. The security assessment of a system includes analysis that considers the assets of a system, the threats that can cause a security breech, the vulnerabilities and weaknesses that results from these threats, and the countermeasures that can be applied to protect the system.

The notions of safety and security may appear to be different, but they are similar in the sense that:

(i) they concerned with freedom from different types of undesirable incidents. Safety is predominantly concerned with preventing the occurrence of harm to human life, and security prevents unauthorised access to information;

(ii) both define a concept of a risk. The risks to a system are either eliminated or made as low as reasonable practicable using the ALARP principle.

In the context of HISs, the notions of safety and security are inter-related and thus an overlap exists. For instance, a scenario can easily arise in which damage to the information in a system could lead to a consequential hazardous situation for patient treatment.

5.1.3 Dependability

When a system is developed to incorporate the notions of both safety and security, the main aim is to ensure that the system becomes more dependable. Hence, the term dependability can be used to describe the type of systems considered in this CR. This term is often used to describe a system in which reliance can justifiably be placed on the service that it delivers to its users. Dependability is considered to be a generic term because it has been defined as comprising the factors of: reliability, safety, maintainability, availability and security [3], [4]. Thus dependability is quantified in terms of various factors that combine to produce a dependable systems. However, the importance of the these factors will vary between applications. Hence, if this term is to be used within the healthcare domain, then an appropriate technical committee should decide on its exact definition.

5.2 Medical Devices versus HIS's

A wide range of information systems exist in the Healthcare sector. A number of these systems are explicitly covered by existing European directives, such as: Active Implantable Medical Devices Directive 90/385/EEC, Medical Devices Directive 93/42/EEC, and the *In-Vitro* Medical Devices Directive.