# SLOVENSKI STANDARD
# SIST-TS CEN/TS 15260:2006

**01-junij-2006**

---

**Zdravstvena informatika - Klasifikacija nevarnosti izdelkov zdravstvene informatike**

Health informatics - Classification of safety risks from health informatics products

Medizinische Informatik - Klassifikation von Sicherheitsrisiken bei der Benutzung von Medizininformatikprodukten



Informatique de santé - Classification des risques de sureté des produits d'information de santé



**Ta slovenski standard je istoveten z:** **CEN/TS 15260:2006**

---

**ICS:**

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

**SIST-TS CEN/TS 15260:2006** **en**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

**CEN/TS 15260**

March 2006

ICS 35.240.80

English Version

# Health informatics - Classification of safety risks from health informatics products

Informatique de santé - Classification des risques de sûreté des produits d'information de santé

This Technical Specification (CEN/TS) was approved by CEN on 24 October 2005 for provisional application.

The period of validity of this CEN/TS 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 CEN/TS can be converted into a European Standard.

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

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.



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

**Management Centre: rue de Stassart, 36 B-1050 Brussels**



Ref. No. CEN/TS 15260:2006: E

# Contents

Page

## Foreword

This Technical Specification (CEN/TS 15260:2006) has been prepared by Technical Committee CEN/TC 251 “Health informatics”, the secretariat of which is held by NEN.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this CEN Technical Specification: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

# Introduction

In the past health-related software was primarily applied to relatively non-critical administrative functions where the potential for harm to the patient, as distinct from disruption to the organisation, was low. Clinical systems were generally unsophisticated often with a large administrative, rather than clinical, content and little in the way of decision support. Even clinical decision support systems tended to be 'light touch', relatively simple and understandable in their logic and used as a background adjunct to decisions, rather than a major influence on which to rely routinely. That has changed and will continue to change substantially. The nature of these changes will increase the potential for risks to patients.

There have been some high profile adverse incidents related to clinical software e.g. in the area of screening and patient call and/or recall where software malfunctions have resulted in failure to 'call' 'at-risk' patients. Such incidents have not only caused anguish for the many patients concerned but may also have led to premature deaths. The trust of the general public has been severely dented. The scope for screening for diseases is increasing significantly and it is in such applications involving large numbers of subjects that there will be heavy reliance, administratively and clinically, on software to detect normals and abnormals and to 'call' or 'process' those deemed to be at-risk. Such software needs to be safe for purpose.

There is mounting concern around the world about the substantial number of avoidable clinical incidents which have an adverse effect on patients of which a significant proportion result in avoidable death or serious disability [1] [2] [3] [4] [5] [6]. A number of such avoidable incidents involve poor or 'wrong' diagnoses or other decisions. A contributing factor is often missing or incomplete information or simply ignorance e.g. of clinical options in difficult circumstances or cross-reactions of treatments.



It is increasingly claimed that information systems such as decision support, protocols, guidelines and pathways could markedly reduce such adverse effects. If for no other reasons – and there are others – this will lead, and is leading, to increasing utilisation of decision support and disease management systems which inevitably will increase in sophistication and complexity. It can also be anticipated that, due to pressures on time and medico-legal aspects, clinicians will increasingly rely on such systems with less questioning of their 'output'. Indeed, as such systems become integrated with medical care any failure to use standard support facilities may be criticised on legal grounds.



Increased decision support can be anticipated not only in clinical treatment but also in areas just as important to patient safety such as referral decision-making, where failure to make a 'correct' referral or to make one 'in time' can have serious consequences.

Economic pressures are also leading to more decision support systems. The area of generic and/or economic prescribing is the most obvious, but economy in number and costs of clinical investigative tests is another.

Systems such as for decision support have considerable potential for reducing clinical errors and improving clinical practice. For example a large body of published evidence gives testimony to the reduction in errors and adverse incidents resulting from the deployment of electronic prescribing. However all such systems also carry the potential for harm. Harm can of course result from unquestioning and/or non-professional use albeit that designers and suppliers can mitigate such circumstances through, for example, instructions for use, training and on-screen presentation techniques, guidance or instruction. The potential for harm may equally lie in the system design such as:

— poor evidence base for design;

— failure in design logic to properly represent design intentions;

— failure in logic to represent good practice or evidence in the design phase;

— poor or confusing presentation of information or poor search facilities;

— failure to update in line with current knowledge.

Some of these system deficiencies are insidious and may be invisible to the user.

A substantial increase in spending on information management and technology is evident in many national health systems. Associated timetables are often tight and the goals ambitious. This increased spending can be expected to attract new suppliers, some of which may be inexperienced in healthcare processes. Such circumstances could lead to an environment of increased risks to patient well being.

Part of the foreseeable explosion in information and communications technology will be in telemedicine. Many of the health informatics products supporting such applications will be innovative and untried and the distance between clinicians and patients will make the scope for errors greater as well as less evident. Similarly, increasing use of innovative mobile IT devices and their application to new fields is likely to be associated with risks.

Whereas the paperless, film-less hospitals are many years distance, GP practices are heading that way. The inability to fall back on paper and film brings increased reliance on computers and databases. Corruption and loss of data can not only bring administrative chaos but can also significantly affect patient care.

In summary the potential for harm to patients from the use of information and communications technology (ICT) in health applications will rise as the use of ICT in health applications rises; the sophistication of the applications increases and the reliance on ICT grows. There is evidence of increasing concern amongst professionals, and by the public, as incidents of malfunctions of software, leading to adverse health consequences, raise public consciousness.

Consequently a number of health organisations are increasingly focusing on 'controls assurance' standards including those on 'governance' and 'risk management'. An important feature of such controls is the management of risk in the context of harm to patients and deficiencies in the quality of care. These controls will often encompass the purchase and application of health informatics products.



Failures and deficiencies in health informatics products can, of course, have adverse impacts other than causing harm to patients. They may, for example, create administrative inconvenience or even administrative chaos, with a range of impacts on the organisation including financial loss. Harm to a patient may also have a consequent impact on the organisation such as financial loss resulting from litigation. Whereas these adverse organisational impacts will be significant to an organisation they are not the subject of this document unless they result in harm to a patient. For example the failure of a hospitals central patient administration system will certainly cause substantial administrative inconvenience but that adverse impact is not in itself within the scope of this document unless it has the potential to cause harm to a patient (which is possible). It is the potential harm to the patient which is the subject of this document.

The safety of medicines and of medical devices in the EU is assured through a variety of legal and administrative measures and is subject to several EU directives [7] [8] [9]. These measures are backed by a range of safety related standards from a number of sources, both national and international, including the European Standards organisation (CEN), the International Standards Organisation (ISO) and the International Electrotechnical Committee (IEC). Software necessary for the proper application of a medical device (together with some software supplied as an accessory for a medical device but necessary for it to meet its purpose e.g. for in vitro devices) is encompassed by these controls e.g. within EU directives and legislation implementing them. However other software applied to health is not covered. This document is concerned with software applied to health which is not encompassed by EU Directives covering medical devices.

A necessary precursor for determining and implementing appropriate design and production controls to minimise risks to patients from product malfunction or inadequate performance, is a clear understanding of the hazards which a product might present to patients if malfunction or an unintended event should occur and the likelihood of such a malfunction or event causing harm to the patient. Additionally if guidance is to be given to designers and producers of health informatics products as to design and production control (and corresponding standards produced) then it will need to be recognised that the controls necessary for products presenting low risks will not be the same as for those presenting high risks. Controls need to match the level of risk which a product might present to a patient. For these purposes many standards, legislation and specifications dealing with control of risks in design and production, group products in to a limited number of classes or types according to the risk they might present. This document presents a process for such a grouping of health informatics products. It proposes five risk classes. This will facilitate broad screening of generic product types and of individual products to allow different levels of, or rigour in, the application of design and production controls which are matched to risk. Thus the classification proposed may be a precursor for standards on design and production control, where the latter might require a far more detailed, in depth and rigorous risk analysis for a particular product than that required for the broad classification process in this document. Examples of the application of the process for assigning a risk class are given for a number of different types of health informatics products.

By ‘health informatics products’ is meant any health informatics product whether or not it is placed on the market and whether or not it is for sale or free of charge. This document thus covers commercial products as well as, for example, open-source health informatics software and software created for, and used in, only one health organisation such as a hospital.

# 1 Scope

This document is concerned with the safety of patients and gives guidance on the analysis and categorisation of hazards and risks to patients from health informatics products, to allow any product to be assigned to one of five risk classes. It applies to hazards and risks which could cause harm to a patient. Other risks such as financial or organisational are out of scope unless they have the potential to harm a patient.

This document applies to any health informatics product whether or not it is placed on the market and whether or not it is for sale or free of charge. Examples of the application of the classification scheme are given.

This document does not apply to any software which is encompassed within EU Medical Devices Directives [7] [8] [9].

# 2 Normative references

Not applicable.

# 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.



**3.1**
**harm**
death, physical injury and/or damage to health or well being of a patient



**3.2**
**hazard**
potential source of harm

[ISO/IEC Guide 51]

**3.3**
**risk**
likelihood of a hazard causing harm and the degree of severity of the harm

**3.4**
**hazard and risk analysis**
investigation of available information to identify hazards and to estimate risks

**3.5**
**tolerable risk**
risk which is accepted in a given context based on the current values of society

[IEC 61508-4]

**3.6**
**safety**
freedom from unacceptable risk of harm

[ISO/IEC Guide 51]

**3.7**
**risk class**
classification of a health informatics product according to the underlying risk it might present to the safety of patients

**3.8**
**patient**
any person who is subject to, or is utilising, a health informatics product. In this document that shall be taken to include healthy persons where applicable (e.g. a healthy person accessing a knowledge data base to obtain health-related information)

**3.9**
**product**
product comprises the entire entity proffered to a user including instructions for use and where applicable training

**3.10**
**health informatics product**
software proffered for use in the health sector for health-related purposes but excluding software necessary for the proper application of a medical device

## 4 Abbreviated terms

ICT Information and Communication Technologies

## 5 Principles of hazard and risk analysis



Designers and producers of health informatics products should have a clear understanding of the hazards which their product might present to a patient, if it were to malfunction or to cause an unintended event and the degree of likelihood that the hazard might be realised if it were to occur in reasonable circumstances of use. That knowledge is necessary for the extent and nature of the control measures required, and the rigour with which they must be applied, so as to reduce the risk to patients to a tolerable level e.g. through measures such as inherent design features, instructions for use, induction training. What is tolerable will depend on circumstances and the current views of society and regulators.



The essential precursor to this process is to undertake a hazard and risk analysis.

There are a variety of approaches to hazard and risk analysis: all share a set of underlying concepts. Existing standards, guidance and publications tend to focus on particular sectors of activity (e.g. electronic safety systems, aeronautics) or subject areas (e.g. financial risks, risks to property, risks to the security of personal data). As such they need interpretation in the context of health informatics products. This document draws on a variety of sources to keep in line with accepted general principles. The Bibliography provides a list of useful sources of information on the subject. In considering the approach to take for health informatics products, account has been taken of how medical devices are classified and controlled in terms of safety. Annex A addresses this matter. The following presents some of the basic concepts in so far as they are utilised in this document. This section is not intended to cover all aspects of hazard/risk analysis.

The risk to the safety of a patient or patients from a health informatics product will depend on the possible consequence(s) that might result if the product malfunctioned or resulted in an adverse event or events, and the likelihood that such consequence(s) would in fact be realised. Thus risk has two aspects: consequence and likelihood.

Note that ISO/IEC Guide 73 [18] defines risk as the “combination of the probability of an event and its consequence” whereas this standard defines it as “the likelihood of a hazard causing harm and the degree of severity of the harm”. This is for two reasons. The probability that a hazard will be realised might, in some domains, be represented quantitatively as a probability which may be based on historical or experimental failure analysis and incident statistics. That is very unlikely to be the case with health informatics products safety where such statistics and evidence are not available: qualitative judgements are necessary. Whereas probability can of course be qualitatively expressed, the term ‘likelihood’ better conveys that meaning and is

therefore used in this standard. Additionally the standard is focussed only on events that are likely to cause harm to patients and the severity of that harm rather than other events. Thus the definition refers to harm rather than other events in general.

The consequence i.e. harm to the patient(s), may take different forms varying from, for example, death to minor inconvenience. Consequences may be categorised. Such categories need interpretation according to their sphere of application: in this case the application of ICT to health. This document proposes five 'consequence' categories each with a description of its scope (see section 6.2).

The likelihood that a hazard will be realised in reasonably foreseeable circumstances might, in some domains, be represented quantitatively as a probability which may be based of historical or experimental failure analysis and incident statistics. That is very unlikely to be the case with health informatics products safety where such statistics and evidence are not available: qualitative judgements are necessary. This document proposes five likelihood categories each with a description of its scope (see section 6.3).

As noted earlier, the risk to the safety of a patient or patients from a health informatics product depends on the possible consequence(s) that might result if the product malfunctioned or resulted in an adverse event or events, and the likelihood that such consequence(s) would in fact be realised. The level of risks can be represented in a risk matrix where likelihood and consequence are its two dimensions (Table 1).

**Table 1**

| **Likelihood** | **Consequence** | | | | |
|---|---|---|---|---|---|
| | **Worst** | | | | **Least** |
| Highest | 1 | 2 | | | |
| | 3 | | | | |
| | | | | | |
| | | | | | 4 |
| Lowest | | | | 5 | 6 |



Each cell of the matrix thereby represents a level of risk. Thus in the risk matrix above the 25 cells represent 25 risk outcomes which reduce in severity on moving diagonally from top left to bottom right.

Such levels of risk outcomes can be grouped into classes such as:

— Highest risk class would be a group of cells in the top left such as 1, 2 and 3;

— Lowest risk class would be a group of cells in the bottom right such as 4, 5 and 6.

The cells of the risk matrix can thereby be populated with risk classes. Which cells are grouped together in to a class requires consideration of the circumstances within the application sector and the meanings assigned to each category of consequence and likelihood. The aim is to reduce complexity by identifying cells which broadly represent a similar degree of risk to the patient and grouping them in to a class on that premise. Thus a minor consequence with a high likelihood might broadly equate to a worse consequence but with lesser likelihood.

This document proposes five risk classes (see section 6.4).

# 6 Assignment of a risk class to a health informatics product

## 6.1 Introduction

This section proposes categories for consequences arising from hazards, and categories for the likelihood of such consequences being realised, in the context of health informatics products. It further proposes a number of risk classes for health informatics products and relates those classes to the proposed categories of consequence and likelihood through a risk matrix. Annex B demonstrates the application of these proposals to different types of health informatics product.

## 6.2 Assignment to consequence categories

Hazards (potential for harm) which a health informatics product might present to a patient if it were to malfunction or be the cause of an adverse event, shall be determined and the potential consequences of such hazards shall be identified. Each such consequence shall be assigned to one of the following consequence categories:

— catastrophic;

— major;

— considerable;

— significant;

— minor.



Note that it will not be necessary to identify and categorise all possible consequences that could arise. The analysis to identify the realistic consequences and the likelihood of their occurring need be undertaken only to the extent necessary to assign, with confidence, the product to a risk class though the iterative process described in section 6.6.



The consequence categories shall be interpreted as in the Table 2. The descriptions have been created to suit the context of this document, but are consistent with those in other sectors and in other complementary disciplines and approaches [11] [12] [13].

Where there is doubt on the margins of two categories the consequence shall be assigned to the category of worse consequence.