TECHNICAL SPECIFICATION

ISO/TS 29321

First edition
2008-##-##

Health Informatics — Application of clinical risk management to the manufacture of health software

Informatique de santé — Application de la gestion du risque clinique à la fabrication de logiciel de santé

PROOF/ÉPREUVE

Reference number
ISO/TS 29321:2008(E)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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

ISO/TS 29321 was prepared by Technical Committee ISO/TC 215, *Health informatics* in collaboration with Technical Committee CEN/TC 251, *Health informatics*.

Introduction

The threat to patient safety

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. See References [1], [2], [3], [4], [5] and [6]. A number of such avoidable incidents involved 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 of the cross-reaction 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 utilization 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 those for decision support have considerable potential for reducing clinical errors and improving clinical practice, e.g. in the reduction in errors resulting from the deployment of electronic prescribing.

Thus decision support and IT in general can bring substantial benefit to patients. However, unless they are safe and fit for purpose they may also present potential for harm.

Annex A provides some examples of the potential for harm of some health software systems.

Harm can of course result from unquestioning and/or non-professional use although 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:

— flaws in the requirement for the use of the system;

— 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.

Failures and deficiencies in health software products can, of course, have adverse impact other than causing harm to patients. They may, for example, create administrative inconvenience or even administrative chaos, with a range of impacts on the organization including financial loss. Harm to a patient may also have a consequent impact on the organization such as financial loss resulting from litigation. Whereas these adverse organizational impacts will be significant to an organization they are not the subject of this document unless they result in harm to a patient. It is the potential harm to the patient which is the subject of this document.

Controlling the risks

The safety of medicines and of medical devices is ensured in many countries through a variety of legal and administrative measures. In the European Union the safety of medical devices is subject to several EU directives. See References [7], [8], [9] and [37]. These measures are often backed by a range of safety-related standards from a number of sources, both national and international, including the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the Global Harmonization Task Force (GHTF). Some software such as that necessary for the proper application or functioning of a medical device is often encompassed by these legislative controls. Some software may be considered a medical device in its own right. However other software applied to health of a stand-alone nature is not usually covered or is encompassed in a less than clear manner or is not currently a primary focus of some regulatory bodies. Depending on national regulations, examples might be general practitioners'/physicians' computer systems, electronic health records, patient administrative systems, applications of bar coding, for example to identify patients or medicinal products, a range of clinical decision support software, ambulance dispatch systems, call and recall screening software. These matters are complex and changing. For a full analysis see EN TR 15640 [11]. This document is concerned with software applied to health excluding that which is encompassed by medical device controls.

A necessary precursor for determining and implementing appropriate design and production controls to minimize risks to patients from poor design, product malfunction or inadequate performance is a set of safety requirements. These should be derived from an initial set of hazards and require a clear understanding of the risks which a product might present to patients if malfunction or an unintended event were to 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 software 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 may not be the same, or applied with the same rigour, as for those presenting high risks. The controls which are selected need to match both the level and types 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 into a limited number of classes or types according to the risk they might present. Controls are then tailored to the class or type. For medical devices such groupings are well established. For health software in 2006 CEN published EN TS 15260 [10] which, subject to validation of its risk classes in its Table 4, could provide a process for grouping health software based on risk characteristics.

What control measures might be necessary for the safety of health software has been considered by CEN/TC 251 in EN TR 15640 [11]. The latter contains eleven conclusions which are reproduced in Annex B. Conclusion 8 reads:

“If risk management is to be part of the requirements for ensuring the safety of health software products then:

— A new standard, consistent at a high level with the results of ISO/TMB JWG [12], ISO 14971 [13] and ISO 61508 [14], [15], is required specifically for health software products. That standard should embody the concepts in GHTF/SG3/NI5R8 [16] and build on the experience of the use of CRAMM [17] with ISO 17799 (now numbered ISO 27001:2006) [18].

— The new standard should be backed by an implementation guide specific to health software products.”

In the document “Measures for ensuring patient safety of health software (APSOHIP): Proposed next steps” [19], CEN/TC 251 considered this conclusion a priority. This standard addresses Conclusion 8.

Relationship to ISO 14971 and other safety related standards for medical devices

ISO 14971 [13] is widely used throughout the world for compliance with medical device safety regulations. Such regulations for medical devices in most countries encompass software that is necessary for the proper application of a medical device or software that is an accessory to a medical device. In some jurisdictions, medical device regulations also cover some other software. Thus medical device manufacturers have considerable experience in the application of ISO 14971. Many manufacturers, particularly of electrical medical devices, are experienced in the incorporation of software in medical devices, in producing software supporting such medical devices and/or producing software that is a medical device in its own right. A number of these manufacturers may also produce other health software of a type not encompassed by medical device regulations. It would be advantageous to such manufacturers and any regulators if the standard for the application of risk management to health software bore as close a relationship as practicable to ISO 14971. This may in particular be an advantage in circumstances where software which is part of a medical device complying with ISO 14971, interacts with software not controlled as a medical device but compliant with this Technical Specification. Each may contribute a hazard to the other and thus access to the risk analysis for both may be necessary.

For these reasons this Technical Specification takes as its baseline ISO 14971. As far as practicable and appropriate the layout and requirements of the main text of ISO 14971 have been retained. However, most of the annexes to ISO 14971 are clearly not applicable to health software (e.g. deal with biological hazards, *in vitro* devices and characteristics of medical devices) and have therefore been replaced or amended as appropriate.

Wherever appropriate this Technical Specification also takes account of work progressing in IEC/SC62A and ISO/TC 210 on a work item TR 80002 [20] which itself has been drafted in the context of IEC 62304 [21]. It also takes note of the work item IEC 80001 [34].

Health Informatics — Application of clinical risk management to the manufacture of health software

1 Scope

This Technical Specification describes the risk management processes required to ensure patient safety in respect to the manufacture of health software products as defined in 2.17. It does not apply to software which is:

— necessary for the proper application of a medical device;

— an accessory to a medical device;

— a medical device in its own right.

This Technical Specification applies to any health software product whether or not it is placed on the market as an off-the-shelf or configurable product and whether or not it is for sale or free of charge. It is addressed to all manufacturers of health software products as defined in 2.17.

This Technical Specification does not cover the manufacture of non-health software which may be incorporated in health software, for example OTS products such as operating systems, e.g. UNIX (Windows), DBMS or SOUP products. However where a non-health software product such as an OTS or SOUP product is incorporated by a manufacturer into a health software product, this Technical Specification shall apply to the totality of that engineered product and shall include the non-health software product on which it is based.

NOTE 1 The scope is intended to cover health software products that are not controlled by medical device regulations. It is acknowledged that, on the boundary, there are health software products that are encompassed by medical device regulations in some countries but not in others. This matter is considered in detail in the CEN/TR 15640 [11].

NOTE 2 The life cycle of a health software product includes:

— requirements capture and concept development;

— detailed design;

— production;

— software release/marketing;

— deployment;

— use;

— decommissioning.

A manufacturer is responsible for requirements capture and concept development, detailed design, production and software release/marketing and can be responsible for deployments particularly the first “go live” of complex systems. Where a customer contracts out responsibility for IT services to the manufacturer, the latter may also be responsible for use of the application and its decommissioning. This Technical Specification applies to all the life-cycle phases for which the manufacturer is responsible where this will depend on the contractual scope with the customer.

NOTE 3 Failures and deficiencies in software products used in the health environment can, of course, have adverse impacts other than causing harm to patients. They might, for example, create administrative inconvenience with a range of impacts on the organization including financial loss. Harm to a patient may also have a consequent impact on the organization such as loss of reputation and/or financial loss resulting from litigation. Whereas these adverse organizational

impacts will be significant to an organization, they are not the subject of this Technical Specification unless they can result in harm to a patient. It is the potential harm to the patient that is the subject of this Technical Specification.

NOTE 4 Whereas this Technical Specification might well be useful to regulators if health software products were to be regulated or controlled in some formal or informal or voluntary manner whether national, regional or local, it is not the purpose of this document to recommend whether or not health software products should be regulated.

NOTE 5 Guidance on the proper processes to be used by the user community to ensure the patient safety of health software as it is deployed, is given in ISO/TR 29322 [35].

NOTE 6 Throughout this document the term “clinical” is used to make clear that the scope is limited to matters of risks to patient safety as distinct from other types of risk such as financial. The use of the term “clinical” is not be taken to mean that the manufacturer is expected to be involved in clinical decisions affecting the treatment of patients in the direct clinical settings. This Technical Specification however makes clear that decisions about risks to patients posed by a health software product in a clinical environment need to involve appropriate, experienced and knowledgeable clinicians.

2 Terms and definitions

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

2.1
clinical hazard
potential source of harm to a patient

[ISO/IEC Guide 51:1999, definition 3.5]

2.2
clinical risk
combination of the likelihood of occurrence of harm to a patient and the severity of that harm

NOTE Adapted from ISO/IEC Guide 51:1999 (definition 3.2).

2.3
clinical risk analysis
systematic use of available information to identify and estimate a risk

NOTE Adapted from ISO/IEC Guide 51:1999 (definition 3.10).

2.4
clinical risk assessment
overall process comprising a clinical risk analysis and a clinical risk evaluation

[ISO/IEC Guide 51:1999, definition 3.12]

2.5
clinical risk control
process in which decisions are made and measures implemented by which clinical risks are reduced to, or maintained within, specified levels

2.6
clinical risk estimation
process used to assign values to the likelihood of occurrence of harm to a patient and the severity of that harm

2.7
clinical risk evaluation
process of comparing the estimated clinical risk against given risk criteria to determine the acceptability of the clinical risk

2.8
clinical risk management
systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling clinical risk

2.9
clinical risk management file
repository of all records and other documents that are produced by the clinical risk management process

2.10
clinical safety
freedom from unacceptable clinical risk to patients

NOTE Adapted from ISO/IEC Guide 51:1999 (definition 3.1).

2.11
clinical safety case
accumulation, through the life cycle of the health software system, of product and business process documentation and of evidence structured such as to enable a safety argument to be developed to provide a compelling, comprehensible and valid case that a system is, as far as the clinical risk management process can realistically ascertain, free from unacceptable clinical risk for its intended use

2.12
clinical safety case report
report that summarises the arguments and supporting evidence of the clinical safety case at a defined point in the health software's life cycle

2.13
clinical safety management system
organizational structure, processes, procedures and methodologies that enable the direction and control of the activities necessary to meet clinical safety requirements and clinical safety policy objectives

2.14
OTS
off-the-shelf software that is not health software

2.15
harm
death, physical injury and/or damage to the health or well-being of a patient

NOTE Adapted from ISO/IEC Guide 51:1999.

2.16
hazardous situation
circumstance in which a patient is exposed to one or more hazard(s)

NOTE Adapted from ISO/IEC Guide 51:1999 (definition 3.6).

2.17
health software product
software product for use in the health sector for health related purposes but excluding software that is:

— necessary for the proper application of a medical device;

— an accessory to a medical device;

— a medical device in its own right.

NOTE 1 This definition is intended for this Technical Specification only.

NOTE 2 For the purposes of this Technical Specification software includes firmware.

NOTE 3 This definition is intended to cover software products used in the health sector which are not covered by medical device regulations. It is acknowledged that, on the boundary, there are health software products that are encompassed by medical device regulations in some countries but not in others. This matter is considered in detail in EN/TR 15640 [11].

2.18
intended use
use of a product, process or service in accordance with the specifications, instructions and information provided by the manufacturer to customers

NOTE Information provided by the manufacturer includes information relevant to misuse as determined by the risk management processes laid down in this Technical Specification.

2.19
life cycle
all phases in the life of a health software product, from the initial conception to final decommissioning and disposal

2.20
manufacturer
natural or legal person with responsibility for the design, manufacture, packaging or labelling of a health software product, assembling a system, or adapting a health software product before it is placed on the market and/or put into service, regardless of whether these operations are carried out by that person or on that person's behalf by a third party

NOTE A manufacturer can be involved in part of or the whole of the software life-cycle including deployment, use and decommissioning of the software according to the contractual scope with the customer.

2.21
medical device

any instrument, apparatus, implement, machine, appliance, implant, *in vitro* reagent or calibrator, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of:

— diagnosis, prevention, monitoring, treatment or alleviation of disease;

— diagnosis, monitoring, treatment, alleviation of or compensation for an injury;

— investigation, replacement, modification, or support of the anatomy of a physiological process;

— supporting or sustaining life;

— control of conception;

— disinfection of medical devices;

— providing information for medical purposes by means of *in vitro* examination of specimens derived from the human body;

and which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means

NOTE This definition has been developed by the Global Harmonization Task Force (GHTF). However, definitions vary from country to country and the extent to which software is covered by such definitions varies within regulatory environments of different countries. This Technical Specification is intended to cover health software products that are not covered by medical device regulations (see Clause 1). It is acknowledged that, on the boundary, there are health software products that are encompassed by medical device regulations in some countries but not in others. This matter is considered in detail in the EN/TR 15640 [11].

2.22
objective evidence
data supporting the existence or verity of something

NOTE Objective evidence can be obtained through observation, measurement, testing or other means.

[ISO 9000:2005, definition 3.8.1]

2.23
patient
any person who is subject to a health software product

NOTE 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).

2.24
pre-release stage report
stage report produced and signed off by top management, before a health software product is released for distribution or deployment

2.25
post-production
part of the life cycle of the product after the design has been completed and the health software product has been manufactured, prior to its release for use

2.26
post-deployment
part of the life cycle of the health software product after it has been manufactured, released and deployed ready for use

2.27
procedure
specified way to carry out an activity or a process

[ISO 9000:2000, definition 3.4.5]

2.28
process
set of interrelated or interacting activities which transforms inputs into outputs

[ISO 9000:2000, definition 3.4.1]

2.29
product
entire entity of software proffered by a manufacturer to a user including instructions for use and, where applicable, training and other such related services

2.30
product liability
legal liability incurred by a manufacturer, merchant or distributor as a result of injury or damage resulting from the use of a product

NOTE In many countries there is strict liability namely, in essence, the plaintiff in litigation needs only to prove a link to his/her injury or damage and a defective product to be successful. In the EU these matters are addressed in the EU Directive 85/374/EEC [33].

2.31
record
document stating results achieved or providing evidence of activities performed

[ISO 9000:2000, definition 3.7.6]

2.32
residual clinical risk
clinical risk remaining after risk control measures have been taken

NOTE ISO/IEC Guide 51:1999 [30], definition 3.9 uses the term “protective measures” rather than “risk control measures”. However, in the context of this Technical Specification, “protective measures” are only one option for controlling risk as described in 7.2.

2.33
severity
measure of the significance of the possible consequences of a hazard

2.34
stage report
report of a review of the clinical risk management process at a defined stage, to ensure all that is required to be done at that stage has been done, as defined in the clinical risk management plan

2.35
top management
person or group of people who directs and controls a manufacturer at the highest level

NOTE Adapted from ISO 9000:2000 (definition 3.2.7).

2.36
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

[ISO 9000:2000, definition 3.8.4]

NOTE 1 The term “verified” is used to designate the corresponding status.

NOTE 2 Confirmation can comprise activities such as:

— performing alternative calculations;
— comparing a new design specification with a similar proven design;
— undertaking tests and demonstrations;
— reviewing documents prior to issue;
— checking that requirements have been addressed.

3 Abbreviated terms

For the purposes of this document, the following abbreviations apply.

EU European Union

DBMS Database Management System (software)

GHTF Global Harmonization Task Force

GP General practitioner

OTS off the shelf

SOUP Software of Unknown Provenance

4 General requirements for effective clinical risk management

4.1 Clinical risk management process

The manufacturer shall establish, document and maintain throughout the life cycle an ongoing process for identifying clinical hazards associated with a health software product, estimating and evaluating the associated clinical risks, controlling these risks, and monitoring the effectiveness of the controls throughout the life cycle. This process shall include the following elements:

- context, requirements and scope identification;
- creation of clinical risk management plan;
- setting the requirements for and defining the competencies of personnel;
- clinical hazard identification;
- clinical risk analysis;
- clinical risk evaluation;
- clinical risk control;
- residual clinical risk acceptance;
- creation of clinical safety case report(s);
- post deployment monitoring;
- post-production maintenance of clinical risk management process.

Annex F gives an example of the necessary components of a generic risk management process.

4.2 Management responsibilities

Top management shall provide evidence of its commitment to the clinical risk management process by:

- ensuring the provision of sufficient resources;
- ensuring the assignment of suitably qualified and experienced personnel (see 4.3) for clinical risk management.

NOTE 1 It is good practice for the top management team to appoint a suitably and sufficiently independent safety function to oversee the effective operation of risk management practices.

Top management shall:

- define and document the organization's risk management policy including criteria for establishing clinical risk acceptability; this policy shall ensure, where applicable, that criteria are based upon national or regional regulations and relevant International Standards, and take into account available information such as the generally accepted state of the art and known stakeholder concerns;
- ensure that a suitably staged approach is taken for the life cycle of the manufacturer's product such that the risk management process can be efficiently and effectively applied; at each stage, top management shall sign off the appropriate stage report (see Clause 9);