TECHNICAL REPORT

ISO/TR 29322

First edition
2008-##-##

Health informatics — Guidance on the management of clinical risk relating to the deployment and use of health software systems

Informatique de santé — Directives relatives à la gestion du risque clinique lié au déploiement et à l'utilisation des systèmes de logiciel de santé

PROOF/ÉPREUVE

Reference number
ISO/TR 29322:2008(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

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

ISO/TR 29322 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 (a substantial percentage of clinical incidents are related to missing or incomplete information).

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 reason – and there are others – this is leading to increasing deployment and use of increasingly complex health software systems, such as for decision support and disease management. It can also be anticipated that, due to pressures on time and to medico-legal aspects, clinicians will increasingly rely on such systems, with less questioning of their "output", as a "foreground" part of care delivery rather than as a "background" adjunct to it. Indeed, as such systems become integrated with medical care, any failure by clinicians to use standard support facilities may be criticised on legal grounds.

Increased use of such systems is not only in clinical treatment but also in areas just as important to patient safety, such as referral decision-making. 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 achieving economy in the number and costs of clinical investigative tests is another.

Thus the use of health software and medical devices in increasingly integrated systems, e.g. networks, can bring substantial benefit to patients. However unless they are proven to be safe and fit for purpose they may also present potential for harm or at least deter clinical and other health delivery staff from making use of them, to the ultimate detriment of patients. Annex A provides some examples of the potential for harm.

Harm can of course result from unquestioning and/or non-professional use, although the manufacturers of health software products, and those in health organizations deploying and using such products within systems, can mitigate such circumstances through, for example, instructions for use, training and on-screen presentation techniques, guidance, warnings or instructions.

Some of these system deficiencies are insidious, may be invisible to the end user and are typically out of the sole control of either the manufacturer or the deploying health organization.

Failures and deficiencies in health software systems 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 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, 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 medical devices is ensured in many countries through a variety of legal and administrative measures which bear on manufacture. In the European Union, the safety of medical devices is subject to several EU directives, see References [7], [8], [9] and [36]. 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 others. 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, there is software applied to health whose manufacture is not covered or is encompassed in a less than clear manner or is currently not a primary focus of some regulatory body. Thus there is health software whose safety in manufacture is not ensured by regulatory controls as a precursor to deployment and use.

This Technical Report applies to deployment and use to which such regulatory controls do not apply. Nevertheless, ensuring safe deployment and use of health software is greatly assisted if the software's manufacture has been conducted in conformance with relevant standards within or without the regulatory environment (see 4.1).

A necessary pre-cursor for determining and implementing controls to minimize risks to patients, from a health software systems that is manufactured and then deployed and used within a health organization, is a clear understanding of the risks which the deployed system 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 deployers and users of health software products then it will need to be recognised that the controls necessary for products presenting low risks are unlikely to be the same, or applied with the same rigour, as for those presenting high risks. The controls that are selected need to match both the level and types of risk that a product might present to a patient when deployed.

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 10 reads:

"Standards for ensuring the safety of health software in the user environment should be addressed."

In the document "Measures for ensuring patient safety of health software (APSOHIP): Proposed next steps" [19], CEN/TC251 considered this conclusion a priority. This Technical Report addresses that conclusion.

A companion Technical Specification ISO/TS 29321 [33] provides processes and other mechanisms for use by health software product manufacturers, whether these be commercial entities or internal providers. Users of this Technical Report can, and should, place a greater degree of reliance upon commercial health software products that are manufactured and provided to them in accordance with ISO/TS 29321, than those that are not.

Relationship to Medical Devices

ISO 14971 [13] is widely used throughout the world for compliance with medical device manufacturing 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, regulations also cover some other software. Thus medical device manufacturers have considerable experience in the application of ISO 14971 and many manufacturers, particularly of electrical medical devices, are now also involved in the manufacture of health software and it can be reasonably assumed that their approach to patient safety will be equally applicable to health software.

It is clearly advantageous to manufacturers, any future regulators of health software, and especially to those deploying and using such software, if the standard for the application of risk management to health software bears as close a relationship as practicable to ISO 14971. This may in particular be an advantage in circumstances where software that is part of a medical device complying with ISO 14971 or ISO/TS 29321, interacts with software not controlled as a medical device but compliant with this Technical Report. Each may contribute a hazard to the other and thus access to the risk information for both may be necessary.

For these reasons this Technical Report takes as its baseline ISO/TS 29321, that in turn was based upon ISO 14971 for the same reasons. As far as practicable and appropriate the layout and requirements of the main text of ISO 14971 have been retained in both this Technical Report and in ISO/TS 29321. As most of the annexes to ISO 14971 are clearly not applicable to health software, and especially to its deployment and use, these have been replaced or amended as appropriate.

Health informatics — Guidance on the management of clinical risk relating to the deployment and use of health software systems

1 Scope

This Technical Report considers the risk management processes required to ensure patient safety in respect to the deployment and use of health software products either as a new system within a health organization or as changes to an existing system's environment.

It is addressed to those persons in health organizations who are responsible for ensuring the safety of health software in health organizations through the application of risk management ("the responsible person" – see definition 2.31). Whilst it is therefore principally addressed to healthcare organizations, it will also prove a useful reference to those involved in the manufacture of health software products. Equally, readers of this Technical Report are recommended also to review ISO/TS 29321 [33] (see 4.1).

NOTE 1 The overall life cycle of a health software system includes its concept realization, design, production, deployment, use and eventual decommissioning. This Technical Report provides guidance to the responsible person for the application of risk management to the last three stages of the life cycle whereas the manufacturer is responsible for the first three stages (by applying ISO/TS 29321). As discussed in 4.1, it is recognised that, depending upon contractual conditions, the manufacturer may be involved in deployment and, in some circumstances, in use and decommissioning. However, the basic processes recommended in this Technical Report are the same as those required of a manufacturer in ISO/TS 29321 so the same processes can be applied throughout and should essentially be applied with the responsible person and manufacturers working together whenever possible. These matters are addressed further in Clause 4.

NOTE 2 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" should not be taken to mean that the persons involved in deployment and use are expected to be involved in clinical decisions affecting the treatment of patients in the direct clinical settings, unless this is consistent with some other aspect of their duties. This Technical Report however, makes clear that the assessment of risks to patients in the deployment and use of health software, and in decisions taken about those risks, needs to involve appropriate, experienced and knowledgeable clinicians.

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 may, 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 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 can result in harm to a patient. It is the potential harm to the patient which is the subject of this document.

NOTE 4 Whereas this document is restricted to health software, the recommended risk analysis should be conducted within the context of any overall risk management system in place in the health organization and any wider health information governance processes.

NOTE 5 This document is restricted to health software but the risk management processes can readily be applied to hardware on which the software runs.

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

NOTE Adapted from ISO/IEC Guide 51:1999.

2.15
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).

2.16
health organization
organization within which health software is deployed or used for a health purpose

2.17
health software product
software product for use in the health sector for health related purposes

NOTE A software product will typically be part of a system.

2.18
health software system
one or more software products from one or more manufacturers who operate together to support a health purpose

2.19
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 should contain references to the specific usages and environment to which the health software product, as part of a system, is intended to be put.

2.20
life cycle
all phases in the life of a health software product, from the initial conception to final decommissioning and disposal

2.21
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 system 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

2.22
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 anatomy or 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 is drawn from the Global Harmonization Task Force (GHTF). Definition varies in detail from country to country.

2.23
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]

2.24
patient
any person who is the subject of a health-related activity which involves a software product

NOTE This definition is for the purpose of this Technical Report only and in that context “patient” is taken to include healthy persons where applicable (e.g. a healthy person accessing a knowledge data base to obtain health-related information).

2.25
post-deployment
that part of the life cycle of the health software system after it has been manufactured, released, deployed and is ready for use by the health care organization

2.26
procedure
specified way to carry out an activity or a process

[ISO 9000:2000, definition 3.4.5]

2.27
process
set of interrelated or interacting activities which transforms inputs into outputs

[ISO 9000:2000, definition 3.4.1]

2.28
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

2.29
record
document stating results achieved or providing evidence of activities performed

[ISO 9000:2000, definition 3.7.6]

2.30
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 Report, "protective measures" are only one option for controlling risk as described in 6.2.

2.31
responsible person
person in a health organization responsible for ensuring the safety of health software in that organization through the application of risk management

2.32
severity
measure of the significance of the possible consequences of a hazard

2.33
top management
person accountable directly to the chief executive or equivalent of a health organization

NOTE For the purpose of the application of this Technical Report, this individual would normally be the clinical director.

2.34
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

NOTE 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 and checking requirements have been addressed.

[ISO 9000:2000, definition 3.8.4]

3 Abbreviated terms

For the purposes of this document the following abbreviations apply.

ALARP As Low As Reasonably Practicable

EU European Union

GHTF Global Harmonization Task Force

GP General practitioner

IT Information Technology

4 General approach

4.1 Relationship between the manufacturer and user health software domains and ISO 14971

There are a variety of measures that need to be taken if patient safety of health software is to be ensured. The measures will require standards to underpin them. What these measures and standards should be is considered in EN TR 15640 [11], the conclusions of which are given in Annex B. The two conclusions most relevant to this Technical Report are:

— Conclusion 8. 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 WG [12], ISO 14971 [13], ISO 61508-3 [14] and ISO 61508-5 [15], is required specifically for health software products. That standard should embody the concepts in GHTF/SG3/N15R8 [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.

— Conclusion 10. Standards for ensuring the safety of health software in the user environment should be addressed.

This Technical Report addresses conclusion 10. However, conclusion 10 is closely linked to conclusion 8 which deals with risk management in manufacture. Thus standards addressing conclusions 8 and 10 also need to be closely related.

When addressing Conclusion 8 regarding clinical risk management in manufacture of health software, account needs to be taken of ISO 14971 [13]. ISO 14971 is widely used throughout the world for compliance with medical device manufacturing 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, regulations also cover some other software and software may be considered a medical device in its own right. Thus medical device manufacturers are well experienced in the application of ISO 14971. Many manufacturers, particularly of electrical medical devices, are involved 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. Thus it would be advantageous to such manufacturers, regulators and those deploying and using such software, if the standard for the application of risk management to health software bore as close a relationship as practicable to ISO 14971. This was deemed practicable since, although ISO 14971 is devoted to medical devices, the essence of its requirements were equally applicable to health software.

Conclusion 8 has now been addressed in ISO/TS 29321 [33] and, for the reasons given above, that 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. Nevertheless one important additional requirement has been added, namely for the manufacturer of health software products to compile a clinical

safety case and to make available to any customer a clinical safety case report which summarises that safety case. For an explanation of a clinical safety case and clinical safety case report see Annex E. The significance of the clinical safety case report is that it comprises the key communication between manufacturer and customer in the context of risk management providing the link between the domains of manufacture and use. This aspect is dealt with in more detail later.

For much the same reasons this Technical Report takes as its baseline ISO/TS 29321 that in turn is based upon ISO 14971. As far as is practicable and appropriate the layout and requirements of the main text of ISO 14971 have been retained on both this Technical Report and ISO/TS 29321. As most of the annexes to ISO 14971 are clearly not applicable to health software, and especially to its deployment and use, these have been replaced or amended as appropriate. Utilization of ISO 14971 in both the standard applicable to manufacturing and this Technical Report for deployment and use, facilitates common processes in both domains and eases hand-over and collaboration between manufacturers and customers particularly in the deployment stage.

When addressing Conclusion 10, regarding risk management in the user domain, it is important to ensure, as far as practicable, that there is a seamless link with risk management in the manufacture domain. Not least of the reasons is that users/health organizations are often involved with the manufacturer in design specification of software products and the manufacturer is often involved with the deployment of health software systems in the user environment. Indeed a typical life cycle for a health software system comprises requirements capture and concept development, detailed design, software development, software verification, software release/marketing, deployment, system validation, use and decommissioning and, depending on the contractual relationship between manufacturer and customer/user, one or other or both may be involved in any of these stages. Thus it is important that any standard on risk management in the user domain have a close relationship with the standard applicable to manufacturer of health software namely ISO/TS 29321 (which in turn is based on ISO 14971 thereby providing the link to software regulated in the context of medical devices).

Thus this Technical Report has the same layout as, and proposes the same risk management processes as, ISO/TS 29321 which in substance means ISO 14971 with the addition of a clinical safety case.

4.2 Relationship with information security

Information security is generally recognised as addressing the implications of breaches of confidentiality and losses of availability and integrity. Whilst the principal concern is about information, security is typically also taken to encompass the systems (hardware and software) on which that information is processed and the environment (human and physical) within which the processing takes place. The strong correlation between clinical safety risk management and information security risk management is therefore clear.

In the construction of this Technical Report therefore, account has also been taken of ISO/IEC 27001 [18], that is founded upon risk management, and of ISO 20856 [34], that provides strong recommendations to health care organizations. In some jurisdictions, these International Standards may well have regulatory or legislative support. Whatever may be the case, they will be of significant relevance to those seeking to deploy and to use health software systems.

4.3 Relationship with other elements of clinical and corporate governance

Risk management is an increasingly significant consideration for health care organizations in their drive to be seen to apply good management practices to clinical delivery and to corporate operations, but also to avoid such issues as the spread of hospital-acquired infections, expensive litigation, widespread/vocal dissatisfaction and staff non-co-operation.

Most such subjects rely to a greater or lesser extent upon scenario development, impact and likelihood assessment and selection of controls. As such there will be useful information either available to or available from patient safety risk management for these activities.

Wherever possible, health organizations will want to establish integrated processes to allow coherent analysis and response to the different manifestations of the same underlying problems.