TECHNICAL REPORT

ISO/TR 27809

First edition
2007-07-15

Health informatics — Measures for ensuring patient safety of health software

Informatique de santé — Mesures assurant au patient la sécurité des logiciels de santé

Reference number
ISO/TR 27809:2007(E)

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is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.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 27809 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Introduction

The threat to patient safety

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 organization, 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. This 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 patients concerned but may also have led to premature deaths. The trust of the general public has been severely affected. 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 on software, administratively and clinically, to detect normals and abnormals and to "call" or "process" those deemed to be at-risk. Such software needs to be safe for its purpose.

Chief Executives and others responsible for healthcare organizations need to recognise that:

— health software products have the potential to harm patients;

— this potential is growing as the complexity of implementations grows;

— healthcare organizations are increasingly reliant on health software products.

This means that, unless these risks are recognised and controlled, harm to patients may result with consequent damage to the reputation of a health organization and substantial financial consequences in terms of legal damages.

There is mounting concern around the world about the substantial number of avoidable clinical incidents that have an adverse effect on patients of which a significant proportion result in avoidable death or serious disability. See Bibliography [1] [2] [3] [4] [5] [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 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. 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.

Failures and deficiencies in health software 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 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. For example, the failure of a hospital's 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 that 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. 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 Committee (IEC) and the European Committee for Standardization (CEN). Some software such as that necessary for the proper application or functioning of a medical device is often encompassed by these legislative controls. However, other software applied to health of a stand-alone nature is not usually covered or is encompassed in a less than clear manner. 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 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 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 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 into a limited number of classes or types according to the risk they might present. Controls are then tailored to the class or type. This document follows that philosophy.

There is a wide range of controls which might be exerted on the design, development, production, distribution, installation, up-grading/version control/up-dating of a health software product, etc. This document starts with considering how those controls are applied to medical devices and offers practical solutions how to adapt them to health software products.

Health informatics — Measures for ensuring patient safety of health software

1 Scope

This Technical Report considers the control measures required to ensure patient safety in respect to health software products. It does not apply to software which is:

— necessary for the proper application of a medical device or

— an accessory to a medical device or

— a medical device in its own right.

This Technical Report is aimed at identifying what standards might best be used or created, and their nature, if health software products were to be regulated or controlled in some other formal or informal or voluntary manner whether national, regional or local. However, it is not the purpose of this Technical Report to recommend whether or not health software products should be regulated.

This Technical Report applies to any health software product whether or not it is placed on the market and whether or not it is for sale or free of charge. It is addressed to manufacturers of health software products.

NOTE The scope is intended to cover health software products which are not, in practice, covered by medical device regulations. Annex A considers this matter in detail. This Technical Report acknowledges that, on the boundary, there are health software products which are encompassed by medical device regulations in some countries but not in others and that some definitions of medical devices may appear to cover health software products in general but in practice do not.

2 Terms and definitions

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

2.1
harm
death, physical injury and/or damage to health or well being of a patient

2.2
hazard
potential source of harm

[ISO/IEC Guide 51:1999] [7]

2.3
health software product
software product for use in the health sector for health related purposes but excluding software which is:

— necessary for the proper application of a medical device or

— an accessory to a medical device or

— a medical device in its own right.

NOTE For the purposes of this document software includes firmware.

2.4
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 himself or on his behalf by a third party

2.5
medical device
any instrument, apparatus, implement, machine, appliance, implant, *in vitro* reagent or calibrator, software, material or other similar or related article:

a) 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 or of a physiological process;

— supporting or sustaining life;

— control of conception;

— disinfection of medical devices;

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

b) 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 intended function by such means

NOTE This definition is drawn from the Global Harmonization Task Force (GHTF) [8]. However, with regard to the coverage of software, there are some differences in definition in different countries which this Technical Report addresses in Annex A.

2.6
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).

2.7
product
entire entity of software proffered to a user including instructions for use and, where applicable, training

2.8
risk
combination of the probability of occurrence of harm and the severity of that harm

[ISO/IEC Guide 51:1999, definition 3.2] [7]

2.9
safety
freedom from unacceptable risk

[ISO/IEC Guide 51:1999, definition 3.1] [7]

3 Abbreviated terms

— CDRH: Center for Devices and Radiological Health (of the FDA)

— EU: European Union

— FDA: USA Food and Drug Administration

— GHTF: Global Harmonization Task Force

— TS: Technical Specification

4 Outline of the issues

If, as it appears, the risk to patients from health software products is current and may increase over time (see Introduction) then the question arises as to how to minimize those risks.

Control over risks can be exerted in many different ways and at different levels. Locally this might be achieved through requirements laid down at the time of purchase, e.g. through tender documentation. Regional or national controls might be imposed through codes of practice or formal guidance. Nationally or trans-nationally, e.g. across the EU, controls might be implemented through a legislative structure. This Technical Report does not assume any particular means of control, but recognises that, whatever the means, requirements will need to be backed by standards. It is those standards which are the focus of this Technical Report.

Risks from medical devices are minimized in many countries through legislature controls aimed at matters such as design, production, distribution and other elements of a device's life-cycle. These controls and the standards/requirements on which they are based exhibit substantial similarities from country to country (see Clause 5) and are extensive, well-documented and established. Software that is necessary for the proper application of a medical device, or is an accessory, is generally encompassed by these medical device legislature measures. Software may, in certain circumstances, be considered as a medical device in its own right albeit what might be considered a medical device in one country may not be so considered in another. Risks from software covered by medical device controls can be considered as already controlled and minimized and are thus not the subject of this Technical Report (see Clause 1).

However, there is at present a great variety of software available and in use which is not encompassed by medical device legislation/controls. 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 or a range of clinical decision support software, ambulance dispatch systems, call and recall screening software: i.e. health software products as defined in this Technical Report. It is “products” such as these which concern this Technical Report albeit that, because of the variations around the world in the definitions of medical devices and their practical implementation, it is possible that one or more of the examples might, in practice, be regulated somewhere as a medical device (see Clause 1).

Insofar as software is controlled through medical device legislation and associated requirements/standards, it would appear sensible to consider whether the same control mechanisms and requirements should and/or could be applied to software which is not controlled in this way. This is particularly the case because of a range of software which lies on the boundary (see Clause 6). It makes little sense to have health software controlled in a number of different ways if some harmonization is practicable. This Technical Report examines that possibility.

The controls exerted in the context of medical devices mainly depend on the potential risk, which a device is perceived to present to a patient or on the clinical experience already available with this product. In that respect devices are classified, and controls vary according to the class into which a device falls. Clearly, it would be unreasonable to apply the same controls, with the same rigour, to all devices when some devices could present little, if any, risk to a patient and others could present a very serious risk including death.

If the same philosophy is to be applied to health software products then it would be necessary to classify them according to the risk they might present to a patient. Clause 7 considers how best to classify health software products including consideration of medical device classification procedures to assess whether they would be suitable.

There is a variety of control measures that are applied to medical devices according to their class such as various registration requirements, quality systems, design control and risk management. Clause 8 examines these in the context of health software and considers what standards might underpin them for health software.

Finally, there will be a continuing need to develop standards relevant to specific risks (see Clause 9).

5 General position on medical device controls

Software that is necessary for the proper application of a medical device or that is an accessory is encompassed by medical device controls in a number of countries. Indeed in some defined circumstances in some countries software may be considered a medical device in its own right. Although such software is outside the scope of this document, it is useful to review the nature of controls over medical devices in different countries, with a particular eye on software aspects. The purpose is to assess whether the controls exerted on medical devices in general, and software in particular, can be suitably applied also to that software not encompassed by such medical device controls, i.e. to health software products.

Annex A considers the position in the EU, Australia, Canada, the USA and the GHTF. The annex demonstrates that the EU, Australia, Canada and the GHTF have adopted, to a large degree, the same legislative approach to, and controls on, medical devices. In practical terms so has the USA. Whereas software aspects are in practice encompassed in similar ways there are differences. Thus software which is necessary for the proper application of a medical device is covered by controls in all of these countries but the extent to which other health-related software is encompassed is different. Whereas the USA has guidance on software which is “contained” in a medical device including “off the shelf” software used in medical devices, there is little other documentation specific to software.

However, whatever the definitional niceties, it is clear that a great deal of software in the context of health software products is not, in practice, encompassed by controls albeit that some consideration is being given to changing this. There are nevertheless some problems on the boundaries between medical devices and health software products.

6 The border between health software products and medical devices

Software that is necessary for the proper application of a medical device, or an accessory of it, is clearly regarded as encompassed by medical device regulatory controls in the EU, Australia, Canada, the USA and the GHTF. Some software will be a medical device in its own right.

Software can be an essential integral part of a medical device (for example part of a pathology analyser providing automation of the analytical process) or an accessory providing additional functions (for example an extra software module, supplied separately, which increases the testing ability or range) or it can process data independently of the medical device.

Software in a laboratory information system can allow data from the analyser to be stored and transmitted to other remote workstations. If it processes the data so as to yield information that would not otherwise be available, and thus it provides or assists with the diagnosis, monitoring, prevention or treatment of a medical condition, it is likely to count as an accessory to a medical device. If on the other hand it is not required by the analyser for normal function, and only stores or transmits data that could be obtained from the analyser(s) directly, without using the software, it is likely to fall outside the regulatory framework for medical devices. In each case, however, the regulatory status could differ between one country and another, or could change with time as new or revised regulations are introduced.

What items of software are medical devices in their own right does not appear clear from the definitions of a medical device used in different countries. Even where, as in GHTF, the medical device definition explicitly includes software, its scope is restricted by the defined functions (see Annex A.3).

Thus, there is health software which may or may not be covered by medical device regulations depending on definitional aspects in different countries. This boundary will shift over time.

What is clear is that a great deal of software (health software products in the context of his document) is not covered by medical device regulations either by design or by practice.

Nevertheless, insofar as some software is encompassed by medical device regulations it makes sense to examine how that software is classified and controlled so as to assess whether the same, or similar, could be applied to software which is not regulated.

7 Classifying health software products

7.1 Options

The controls exerted on medical devices depend on the risk they are seen to present to patient safety. The approach taken for medical devices is to assign every device to one of several classes. The higher the risk represented by the class the more comprehensive and rigorous are the controls for that class.

If measures to ensure patient safety of health software products are also to be proportionate to the risk they might present to a patient, then health software products will also need to be classified according to risk.

The first obvious question is whether health software products can be classified according to the same classification rules as for medical devices. Annex B considers classification of medical devices in different countries and other options and its conclusions follow.

The EU, Australian, Canadian, USA and GHTF classification systems for medical devices are not suitable for health software products.

The FDA CDRH classification of “software in medical devices”, Bibliography [9], and “off the shelf”, Bibliography [10], software could be applied to health software products.

However, ISO/TS 25238:2007 [11] describes the most suitable classification system, subject to validation of its risk classes in its Table 4. It is consistent with the USA, FDA, CDRH approach to “software in medical devices” and “off the shelf” software.

7.2 Conclusions

If controls are to be proportionate to the risk that a product might present to a patient, then health software products will need to be classified according to those risks. Medical device classification systems are not suitable for health software products. The ISO Technical Specification “Classification of safety risks from health software” [11] is deemed the most appropriate, subject to validation of its risk classes in its Table 4.

8 Options for control measures for health software products

8.1 Overview

8.1.1 General

Once health software products have been assigned to a class according to the risk they might present to a patient, the next step is to consider what controls, if any, should be assigned to those classes/risks.

For medical devices the control measures utilized are generally the same in nature in different countries but with differences in naming and detailed content. The following list has been compiled from control measures adopted for medical devices in the EU, Australia, Canada, GHTF and USA and comprises a useful list of options that might also be applied to health software products:

— pre-market notification with or without pre-market approval;

— establishment registration;

— product listing;

— clinical evidence requirements;

— labelling requirements;

— reporting of incidents that may have caused or contributed to death or serious injury;

— quality system or good manufacturing practice requirements with or without inspection;

— design control;

— risk management.

However, it is not the purpose of this Technical Report to examine in detail regulations and control measures. It is also not the purpose of this Technical Report to recommend whether or not health software products should be regulated. This Technical Report is aimed at identifying what standards might be best used or created, and their nature, if health software products were to be regulated or controlled in some other formal, informal or voluntary manner. The control measures are listed therefore solely to allow discussion of those standards which might underpin them if such controls were to be put in place.

Thus, whether pre-market notification, establishment registration or product listing would be deemed necessary for controlling the safety of health software products, is a matter for those responsible for controls. If they were deemed necessary, the content of the documentation/standards would appear straightforward and would not require standards development.

8.1.2 Conclusions

If pre-market notification, organization and product registration are required, they do not appear to require standards development.

8.2 Labelling and documentation

8.2.1 General

Labelling can cover not just matters on the immediate container of any product but also to “posters, tags, pamphlets, circulars, booklets, instruction books, direction sheets”, etc. It may also cover advertising.

Labelling requirements for health software products will have much in common with medical devices, and the standard EN 1041 [13] for medical devices should be reviewed to see if it is fully applicable. However, there may be requirements which would be characteristic of health software products, e.g. hardware and interface requirements. In a world where interoperability and interworking of health software products is of increasing importance and where interoperability failures could have serious consequences, a full and accurate statement on the characteristics of a health software product will be important. Such a statement could be said to fall within the broad definition of labelling. It should be recognised that system characteristics, documentation about the product and instructions for use may all be provided on line and not delivered direct to the user as with paper.

8.2.2 Conclusions

A standard on the minimum information required for documentation of the characteristics of health software products could be advantageous particularly regarding those characteristics that are significant for interworking and interoperability. The standard for medical devices EN1041 [13] should be reviewed to assess whether there is a need for a standard on general labelling of health software products.

8.3 Clinical evidence

8.3.1 General

Pre-market approval is predominantly aimed at high risk medical devices and may include the submission of clinical data to support claims made for the device. In Australia, regulations require a medical device of any class to have clinical evidence that is appropriate to its use and classification.

It would be a matter of debate whether controls on classes of health software products representing the highest risks should include submission of clinical data. Of significance in such consideration would be that the safety of, for example, clinical decision support products (some of which would be in classes representing the highest risk), will depend on the soundness and currency of the clinical evidence which lies at the foundation of decision support algorithms and pathways. Regarding the latter, clinical evidence can be regarded in two contexts:

— evidence of the validity of the clinical data supporting decision support and the way the software utilizes that evidence;

— clinical evidence drawn from use of the product in the field, e.g. in limited controlled applications.

ISO 14155 [14] on clinical investigation of medical devices for human subjects could have application here.

8.3.2 Conclusions

If the submission of clinical evidence forms part of the controls over safety of health software products, a standard in the form of guidelines would appear to be warranted, tailored to the characteristics of health software products such as decision support. Such a standard should cover both clinical evidence regarding the validity of data underpinning decision support and its use by the software plus clinical evidence drawn from use of the product. In that context, ISO 14155 [14] should be reviewed for its applicability.

8.4 Incident reporting

8.4.1 General

A requirement for medical devices is the reporting of incidents that may have caused or contributed to death or serious injury to a patient.

If such a control measure were required for health software products, electronic reporting could be anticipated. A standard on incident reporting for health software products should therefore be considered. There are documented examples from which to draw, such as:

— ISO/TS 19218:2005 [15];

— the GHTF for medical devices [16];

— FDA MedWatch;

— the general reporting requirements of the UK National Patient Safety Agency [17];

