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)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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

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];

- the work in ISO TC 215 Pharmacy and Medication Business Working Group (WG 6) which is drafting a standard on the electronic reporting of adverse drug reactions (Bibliography [18]) which itself is based on national and international documentation.

8.4.2 Conclusions

A standard for electronic reporting of adverse incidents involving health software products should be considered.

8.5 Quality systems

8.5.1 General

At the heart of any controls on health software products, particularly those in classes representing highest risk, will be a requirement for quality systems. Whereas a standard on quality systems (such as ISO 9000 series) may encompass design control and risk management, they are unlikely to cover these aspects in the detail required. Thus, in the medical device field there are separate standards for quality systems, design control and risk management. The same would probably apply to health software products.

Quality systems can be very effective in ensuring that final products are consistent in their quality but if the original design is poor the danger is that, whilst all the final products will be consistently the same, they will all be consistently poor. Thus, essential features of good quality systems are design control which is considered in 8.6 and the requirement for risk analyses and risk management or mitigation which is considered in 8.7.

Whereas quality systems for health software products will share many of the characteristics of those for medical devices (and products in general), there are existing standards applicable to software which might be more suitable as a baseline. The following considers a number of those of significance. In general they cover matters such as:

- planning product realization such as software life cycle, quality planning, customer-related processes, design control and risk management;
- documentation such as quality manual and control of documents and records;
- management responsibility including management commitment, customer focus, quality policy and quality management system planning;
- allocation of responsibilities and authority;
- communication;
- resource management including competence, awareness and training and the work environment;
- management reviews.

8.5.2 Quality system standards specific to medical devices

Many manufacturers of medical devices have implemented a quality system as a way of satisfying legislative controls.

In most European countries, manufacturers of medical devices have implemented a quality system as a way of satisfying an EU medical devices directive (Bibliography [19]). However, in line with the EU's stance on New Approach Directives (Bibliography [20]), it refers to an assumption of conformity if the manufacturer's quality system complies with “harmonized standards” but does not name them. However, in a listing of guidance on medical device directives (Bibliography [21]), the entry relating to quality systems refers to documents from GHTF.

GHTF guidance was, until June 2005, contained in the document “Guidance on Quality Systems for the Design and Manufacture of Medical Device” [22]. This was in turn based on ISO 9001 (1994 version) [23]. In 2005 this guidance was withdrawn in favour of ISO/TR 14969:2004 [24] in the drafting of which GHTF participated. This Technical Report is, in itself, again firmly based on ISO 9001.

In the USA, Good Manufacturing Practice requirements are set out in the Quality Systems (QS) Regulations [25]. The preamble describes the public comments received and the FDA responses. Within the latter it is made clear that the requirements are substantially based on ISO 9001:1994 [23] and were drawn up in close collaboration with the GHTF. The FDA Medical Devices Quality System Manual for Small Entities Chapter 2 “Quality Systems”[26] similarly states that the GMP requirements “are harmonized with ISO 9001:1994 and ISO 13485 [27]” (which in itself is based on ISO 9001).

The situation in Australia and Canada is similar. Their QS requirements for medical devices are also based on the ISO 9000 series.

Clearly, if health software products were to be subject to controls regarding quality management systems, any standard should be based on ISO 9001:2000 [28]. The question that arises is whether there already exists such a standard which might be directly applied.

The standards applicable to medical devices are obvious candidates. As already noted, the standard referred to in the context of the EU Medical Devices Directive is the GHTF Guidance on Quality Systems [22] which has been withdrawn in favour of ISO/TR 14969:2004 “Guidance on the application 0f ISO 13485:2003” [24]. ISO 13485:2003 [27] (“Quality management systems — Requirements for regulatory purposes”) is, as its title makes clear, specifically written for “regulatory purposes” and is dedicated to medical devices. It would not be suitable for health software products for two reasons:

— although its definition of a “medical device” is that of the GHTF and thereby includes “software” (see A.3) it is clearly not written with health software products in mind;

— it is written for “regulatory” purposes, and this Technical Report is not based on the premise that controls will necessarily be regulatory; some of the emissions and amendments to ISO 9001 in ISO/TR 14969:2004 [24] and ISO 13485:2003 [27] may not be warranted in a non-regulatory environment.

Nevertheless, the basic content and requirements would appear to be as applicable to health software products as they are to medical devices.

8.5.3 Quality systems standards specific to software

Another possible approach to a standard for health software products based on ISO 9001 is to examine the ISO 9001-based existing standards that apply to software generally. The obvious candidate is ISO/IEC 90003:2004 “Guidelines for the application of ISO 9001:2000 to computer software” [29].

The latter in turn refers to a number of ISO/IEC standards, particularly ISO/IEC 12207:1995 [30] on “Software life cycle processes”, its 2002 Amendment [31] and its application guide ISO/IEC TR 15271 [32].

ISO/IEC 9003:2004 could be directly applied to health software products and could therefore be the existing standard of choice. Its possible disadvantages would be in a lack of reference to the ISO 9001-based standards for medical devices.

8.5.4 Conclusions

If one of the controls for ensuring the safety of health software products is the requirement for a quality management system, any necessary standards should be based on ISO 9001:2000 [28].

If it is considered that a new standard specific to health software products is required, it should be based upon examination of ISO/IEC 90003:2004 [29]:

— as a possible candidate without amendment or

— as the baseline with possible amendments specific to health software products (taking into account the requirements for medical devices in ISO 13485:2003 [27] and its associated guide ISO/TR 14969:2004 [24].

8.6 Design control

8.6.1 General

Design control is a feature of most legislative approaches.

Insofar as the EU has recommendations on design control it defers to GHTF documents. GHTF guidance was, until June 2005, contained in the document “Design Control Guidance for Medical Device Manufacturers” [33]. In 2005, this guidance was withdrawn in favour of ISO/TR 14969:2004 [24] “Quality systems management systems – Guidance on the application of ISO 13485:2003” This essentially replaced 44 pages of guidance with 8 pages in ISO/TR 14969:2004, Clause 7. This has resulted in some loss of advice detail.

Australia and Canada have the same approach as GHTF.

In the USA, the FDA has issued “Design Control Guidance for Medical Device Manufacturers” [34]. It relates to the FDA Regulations 820.30 on “Design Controls” and 4.4 of ISO 9001:1994. It covers the same ground as the GHTF guidance namely:

- design and development planning;
- design input;
- design review;
- design verification;
- design validation;
- design transfer;
- design changes;
- design history file.

Even though produced for a regulatory environment (which this Technical Report does not assume), the substance of these requirements would apply just as well to health software products as to medical devices. Nevertheless, they are not altogether suitable because:

- the examples and text are medical device-orientated and therefore not suited to health software products;
- some of the requirements could usefully be tailored to software;
- more detail relevant to health software products particularly, for example, decision support systems, could be warranted (see below).

Design of decision support systems and later design changes will include underlying decision support algorithms and clinical data. Thus, an e-prescribing system will, for example, provide for alerts on contra-indications for medication for young children or pregnant women and for cross reaction between medications. Such features will be heavily dependent on clinical evidence which will change with time. Deficiencies and failure to keep up to date could have serious and even fatal consequences. Here, strong control over initial design and design change, e.g. updates, will be of paramount importance for safety. Any standard on design control for health software products should therefore deal with these types of feature, e.g. possible requirements for peer review of clinical evidence. Existing standards are inadequate in these respects.

8.6.2 Conclusions

If design control is to be part of the requirements for ensuring the safety of health software products, then a standard specific to health software products should be considered. Whereas such a standard should draw upon the basic requirements of design control standards for medical devices, see Bibliography [24] [33] [34], these should be tailored to health software products and tackle specific needs such as control of algorithms and use of clinical evidence in products like decision support systems.

8.7 Risk management

8.7.1 General

There are many standards relating to risk management which could be candidates for application to health software products. Annex C reviews a number of the most significant in the context of those which are related to:

- "enterprise risk management" processes;
- healthcare products, particularly medical devices;
- other areas such as information security management.

8.7.2 Conclusions

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 the ISO/TMB WG [35], ISO 14971 [36], IEC 61508-3 [37] and IEC 61508-5 [38], is required specifically for health software products. That standard should embody the concepts in GHTF/SG3/NI5R8 [39] and build on the experience of the use of CRAMM [40] with ISO/IEC 17799 [65].
- The new standard should be backed by an implementation guide specific to health software products.

9 Standards relevant to risks of a particular nature

9.1 General

A particular health software product, or health software products in general, may be subject to risks of a particular nature. Examples which would apply to most health software products and for which there are ISO and/or CEN standards specific to health software products are:

- security in the context of protection of personal information;
- authentication of healthcare professionals;
- the correct unambiguous identification of patients.

9.2 Conclusions

Wherever risks of a particular nature are addressed by standards, products should be designed to comply with them.

10 Observation on safety and risks in the user domain

10.1 General

This Technical Report is limited to ensuring the safety of health software products in the manufacturing domain (which includes design and development). However even if safety has been ensured in manufacture it is recognised that, when health software is implemented and used in the user domain, e.g. in a hospital or with a general practitioner, new risks can emerge. This is particularly so where health software from different suppliers is expected to interoperate and interconnect, whether directly connected or networked, and to do so with interfaces with medical devices that embody software. This aspect of safety will need to be addressed.

10.2 Conclusions

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

11 Taxonomies

11.1 General

What comprises a health software product lacks clarity and this needs to be addressed by a taxonomy (structured list) of health software. Similarly, for reporting of adverse events an underpinning taxonomy would be beneficial, e.g.:

- health software product (e.g. medication decision support);
- processes (medication dispensing);
- outcomes (allergic reaction or severe harm).

11.2 Conclusions

A taxonomy of health software products and a taxonomy to underpin reporting of adverse events should be produced.

12 Summary of conclusions

If health software products are to be regulated or controlled formally or informally at national, regional or local level, the controls will need to be founded on standards. This Technical Report considers the standards needed and their nature. The conclusions are as follows.

1) 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.

2) If pre-market notification, organization and product registration are required, they do not appear to require standards development (see 8.1).

3) 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 (see 8.2).

4) The submission of clinical evidence might be required for some health software products, e.g. those of highest risk of the nature of decision support. If so, a standard in the form of guidelines specific to health software products, would be desirable. 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 (see 8.3).

5) Incident reporting may be regarded as necessary, in which case a standard on electronic reporting of adverse incidents involving health software products should be considered (see 8.4).

6) If one of the controls for ensuring the safety of health software products is the requirement for a quality management system (see 8.5), any necessary standards should be based on ISO 9001:2000 [28]. If it is concluded that a new standard specific to health software products is required, it should be based upon examination of ISO/IEC 90003:2004 [29]:

   — as a possible candidate without amendment or

   — as the baseline with possible amendments specific to health software products (taking into account the requirements for medical devices in ISO 13485:2003 [27] and its associated guide ISO/TR 14969:2004 [24].

7) If design control is to be part of the requirements for ensuring the safety of health software products, then a standard specific to health software products should be considered (see Clause 10). Whereas such a standard should draw upon the basic requirements of design control standards for medical devices, see Bibliography [24] [33] [34], these should be tailored to health software products and tackle specific needs such as control of algorithms and use of clinical evidence in products like decision support systems.

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 the ISO/TMB WG [35], ISO 14971 [36], IEC 61508-3 [37] and IEC 61538-5 [38], is required specifically for health software products; that standard should embody the concepts in GHTF/SG3/NI5R8 [39] and build on the experience of the use of CRAMM [40] with ISO/IEC 17799 [65];

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

9) Wherever risks of a particular nature are addressed by standards, products should be designed to comply with them.

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

11) A taxonomy of health software products and a taxonomy to underpin reporting of adverse events should be produced.

These conclusions point to a portfolio of standards necessary to ensure the safety of health software products. However, it may not be necessary for there to be one standard for each conclusion. Thus, the requirements for design control and risk management might be part of a standard on quality systems. What will be necessary is a strategic approach to the whole.

Annex A
(informative)

Position regarding medical devices in different countries

NOTE This review is only for the purpose of this document and seeks to highlight and summarise only those aspects of significance to this document. It should not be used as a definitive guide in any respect or for any purpose (the original documentation and the competent national authorities should be referred to).

A.1 The EU, Australia and Canada

A.1.1 General

The EU, Australia and Canada have, to a large extent, adopted the same legislative approach to, and controls on, medical devices and are therefore considered under the same heading.

A.1.2 The EU

In the EU medical devices are controlled through three directives, namely:

— 90/385/EEC of 20 June 1990 [41] concerning active implantable medical devices;

— 93/42/EEC of 14 June 1993 [19] concerning medical devices;

— 98/79/EC of 27 October 1998 [42] on *in vitro* diagnostic medical devices.

The “active implantable medical device” directive refers to all powered or partial implants that are left in the body, e.g. heart pacemakers.

The directive “concerning medical devices” covers most other medical devices (not just medical electrical) ranging from, for example, first aid bandages, hip prostheses, X-ray equipment, ECGs, heart valves.

The directive “on *in vitro* diagnostic medical devices” covers any medical device that is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, equipment or system intended for use *in vitro* for the examination of specimens, including blood and tissue donations, derived from the human body. Examples are blood grouping reagents, test kits for pregnancy or for hepatitis B.

For the purposes of the directives, a medical device is defined as:

“any instrument, apparatus, appliance material or other article, whether used alone or in combination, including the software necessary for its proper application, intended by the manufacturer to be used on human beings for the purpose of:

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

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

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

— control of conception

and which does not achieve its principal 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”.

This definition encompasses only software “necessary for the proper application” of a medical device but the definition is likely to change in the near future to recognise some software as a medical device in its own right.

The Medical Devices and the Vitro Diagnostic Medical Devices Directive includes a system of classification whereby the level of regulatory control applied to a device is related to the perceived degree of risk associated with the device.

The controls exerted on a medical device cover matters such as registration of manufacturers and products, requirements regarding design and production, and inspection to ensure requirements are met.

A.1.3 Australia

Australia adopted a new regulatory system for medical devices on 4 October 2002, see Bibliography [43] [44], based on the international regulatory model developed by the Global Harmonization Task Force (see [55]). The latter and the Australian system itself have many similarities with the EU Regulatory Systems. The differences between Australia and the EU, see Bibliography [45] [46], are not significant in the context of this document. Thus the definition of a medical device, the classification systems, the requirements for registration and the control measures are essentially the same as the EU.

As in the EU, software is encompassed only if it is software necessary for the “proper application” of a medical device. Australia has an Australian Register of Therapeutic Goods (ARTG). A word search for “software” and “computer” has revealed only software systems necessary for the proper application of medical devices but no software systems of the nature of health software products in the context of this document (the nearest was Picture Archiving and Communication systems – PACS software). Similarly in the Australian classification system the only software classified was “software for image processing”.

A.1.4 Canada

In Canada medical devices are controlled through the Medical Devices Regulations [47] and the sections of the Food and Drugs Act applicable to medical devices. Health Canada is responsible for managing national compliance and enforcement, see Bibliography [48].

Although the definition of a medical device does not include mention of software, the Medical Devices Regulations include the requirement that:

— “If a medical device consists of or contains software, the software shall be designed to perform as intended by the manufacturers, and the software shall be validated”.

Medical devices and *in vitro* diagnostic devices are classified through rules developed so that they are “harmonized” with the EU device classification rules and the device classifications of the USA, see Bibliography [49] [50]. Classification for medical devices is substantially the same as Australia and the EU. Software is not explicitly mentioned except software that is associated with or dedicated to certain devices, e.g. active therapeutic and diagnostic devices, those emitting radiation, drug delivery and anaesthetic equipment. Software is also mentioned in the context of that which is intended to be used with *in vitro* diagnostic devices.

The Canadian Therapeutics Product programme provides a keyword index to assist manufacturers in verifying the class of medical devices, see Bibliography [51]. Although this includes a category “computer” the descriptions of systems are all associated with particular types of medical devices. Therefore no software is encompassed by controls, which is of the nature of health software products in the context of this document.

A.2 USA

In the USA medical devices are controlled by the Food and Drug Administration (FDA) and its Center for Devices and Radiological Health (CDRH).

As defined by the Federal Food Drug and Cosmetic Act a medical device is:

“an instrument, apparatus, implement, machine, contrivance, implant, *in vitro* reagent, or other similar or related article, including a component part, or accessory which is:

- recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them, intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or intended to affect the structure or any function of the body of man or other animals, and which does not achieve any of its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes.”

Software which is “contained” in a medical device including “off the shelf” software used in medical devices is encompassed by these controls, see Bibliography [52] [53]. Guidance on General Principles of Software Validation [54] applies to:

- software used as a component, part, or accessory of a medical device;
- software that is itself a medical device (e.g. blood establishment software);
- software used in the production of a device (e.g. programmable logic controllers in manufacturing equipment);
- software used in implementation of the device manufacturer's quality system (e.g. software that records and maintains the device history record).

It can thereby be taken that medical device controls apply to software as defined above.

An uncertain point is what software constitutes a medical device in itself. Software that is encompassed by the definition of a medical device clearly would be. However, health software products in the context of this document could not in essence be described as “an instrument, apparatus, implement, machine, contrivance, implant, *in vitro* reagent, or other similar or related article including part, or accessory”. On the other hand, it might have one of the functions in the definition of a medical device such as “intended for use in the diagnosis of disease or other conditions”. Examination of the FDA/CHRA Product Codes and the scope of “Classification Device Panels” does not resolve the matter. Whether or not software in the sense of health software products could be described as a medical device, in practice very few health software products in the context of this document seem to be regulated software.

However, whether or not this is the case, the purpose of examining the medical device regulations is to determine whether any software in relation to medical devices is controlled and subject to guidance, etc., which could be applicable to software which is not controlled, i.e. to health software products. In the USA there is such guidance and controls which could be considered (e.g. see B.3).

The USA system for classifying medical devices, although different in some respects, is essentially the same as that in the EU, Australia, Canada and the GHTF, at least in the context of this document. However, FDA guidelines relating to software contained in medical devices (see Bibliography [52]) includes a system for classifying such software according to risk or “level of concern”. This classification is considered further in B.3 in relation to health software products.

A.3 The Global Harmonization Task Force (GHTF)

The GHTF is a voluntary group of representatives from national medical device regulatory authorities and regulated industry. Its purpose is to encourage convergence in regulatory practices related to ensuring the safety/effectiveness/performance and quality of medical devices. Through its five study groups it publishes guidance, some of which is relevant to this document.

The GHTF "harmonized" definition of a medical device, see Bibliography [8], is as follows:

"Medical device means 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".

This differs significantly from the definitions in the EU, Australia, Canada and USA in that "software" is explicitly defined as a medical device rather than being encompassed as necessary for the application of, or accessory to, a medical device. However, the software covered is restricted by the bulleted functions. Clearly many health software products would not be embraced by these functions and thereby would be out of scope. However, some would be covered, e.g. "software for the specific purpose of diagnosis of disease".

The GHTF has proposed a document on the "Principles of Medical Devices Classification" [55]. It proposes four classes. The only explicit reference to software is as follows:

"While most software is incorporated into the medical device itself, some is not. Provided such stand-alone software falls within the scope of the definition for a 'medical device', it should be classified as follows:

— where it drives or influences the use of a separate medical device, it will have the same class as the device itself;

— where it is independent of any other medical device, it is classified in its own right using the rules in Clause 8."

However, the sixteen rules in Clause 8 make no further mention of software in the rules themselves or the examples. Although the rules are based on the risk which a medical device might present to a patient, the risk is not defined in terms of consequence; e.g. injury but non-stated, implied seriousness of consequence based, for example, on whether a device is invasive or not. In that sense it is essentially the same as the classification systems in the EU, Australia, Canada and the USA.

Annex B
(informative)

Analysis of classification procedures

NOTE This review is only for the purpose of this document and seeks to highlight and summarise only those aspects of significance to this document. It should not be used as a definitive guide in any respect or for any purpose (the original documentation and the competent national authorities should be referred to).

B.1 EU, Australian, Canadian and GHTF medical device classification

Whereas there are some differences, the system of classifying medical devices in the EU, Australia and Canada are, for the purposes of this document, essentially the same. As an illustration the following provides the essence of classifying a medical device in the EU. It draws on a UK MDA Bulletin No. 10 [56].

The EU rules are set out in Annex IX of the medical devices directive 93/42/EEC [19]. The directive covers a vast range of products from first-aid bandages and walking frames to CT scanners and non-active implants. Devices covered by the directive are grouped into four classes as follows:

- Class I - generally described as low risk;
- Class IIa - generally described as medium risk;
- Class IIb - generally described as medium risk;
- Class III - generally described as high risk.

The difference between each class rests in the choice of conformity assessment procedures available.

The annex opens with a series of definitions (invasive, active, long-term, etc.) so as to minimize any possible ambiguities. There follows a series of implementing rules which lay down the basic principles, such as “If more than one rule applies to a device, the highest classification stands”.

The rules are a set of broad statements relating to situations, functions, parts of the body treated, properties, etc., rather than a list of products, which would require constant updating.

There are 4 groups within the rules as follows:

- Rules 1-4 non-invasive devices;
- Rules 5-8 invasive devices;
- Rules 9-12 additional rules applicable to active devices;
- Rules 13-18 miscellaneous rules for products which merit a higher classification than they might otherwise be assigned.

Whereas it is not the purpose of this Technical Report to examine all these rules in detail, they are clearly not meant for health software products and would not be suitable for them. If they were to be applied, all health software products would be deemed Class I “low risk”. This is clearly not a suitable process.

The Australian (Bibliography [57]) and Canadian (Bibliography [49]) classification processes would be unsuitable for the same reasons as would those of the GHTF (Bibliography [55]).

B.2 USA medical device classification

The classification process in the USA, has a somewhat more extensive definition of risk than “low”, “medium”, “high”, e.g. Class III devices are those that “support or sustain life, are of substantial importance in preventing impairment of human health, or which present a potential, unreasonable risk of illness or injury”. Nevertheless, the classification process, including USA Classification Device Panels, does not appear suitable for health software products for the same reasons as for Australia, Canada and the EU.

B.3 USA FDA guidance related to software classification

The USA FDA has issued guidance on software encompassed by medical device controls. It contains material of significance for this Technical Report.

The “Guidance for the Content of Premarket Submissions for Software contained in Medical Devices” [9] provides a classification of such software based on the “level of concern” it represents to the safety of patients or operators. The nature and extent of documentation required for a premarket submission is then related to the level of concern. The level of concern “refers to an estimate of the severity of injury that a device could permit or inflict, either directly or indirectly, on a patient or operator as a result of device failures, design flaws, or simply by virtue of employing the device for its intended use”. The guidance recognises three levels of concern:

- major: if a failure or latent flaw could directly result in death or serious injury to the patient or operator; the level of concern is also major if a failure or latent flaw could indirectly result in death or serious injury of the patient or operator through incorrect or delayed information or through the action of a care provider;
- moderate: if a failure or latent design flaw could directly result in minor injury to the patient or operator; the level of concern is also moderate if a failure or latent flaw could indirectly result in minor injury to the patient or operator through incorrect or delayed information or through the action of a care provider;
- minor: if failures or latent design flaws are unlikely to cause any injury to the patient or operator.

Serious injury is defined as an injury or illness that:

- is life threatening;
- results in permanent impairment of a body function or permanent damage to a body structure;
- necessitates medical or surgical intervention to preclude permanent impairment of a body function or permanent damage to a body structure.

“Permanent” is defined as “irreversible impairment or damage to a body structure or function excluding trivial impairment or damage”.

A minor injury is one which does not meet the definition of serious.

Of particular significance is the recommendation that the level of concern is assessed “before mitigating any hazard”, i.e. the software device should be assessed as though hazard mitigations had not been implemented.

This recommendation is in essence reflected in FDA guidance on Off-the-Shelf Software Use in Medical Devices [10] which contains the following FDA CDRH view.

“Because the risk estimates for hazards related to software cannot easily be estimated based on software failure rates, CDRH has concluded that engineering risk management for medical device software should focus on the severity of the harm that could result from the software failure. Hazard analysis is defined as the identification of hazards and their initiating causes (IEC 60601-1-4 [67]). Based on the definition of risk analysis in ISO 14971 [36] and EN 1441 [68], hazard analysis is actually a subset of risk analysis; because risk analysis for software cannot be based on probability of occurrence, the actual function of risk analysis for software can then be reduced to a hazard analysis function. Technically speaking, the use of either term risk or hazard analysis is appropriate. However, CDRH has chosen to use the term hazard analysis to reinforce the concept that calculating risk based on software failure rates is generally not justified, and that it is more appropriate to manage software safety risk based on the severity of harm rather than the software failure rates."

The off-the shelf software guidance also proposes a classification based on "level of concern" with definitions which are substantially the same.

These FDA guidance documents point the way to possible approaches for health software products, although it should be noted that the guidance on software in medical devices clearly states that the guidance on "level of concern" applies only to premarket submissions and is "not related to device classification (Class I, II, or III) or to hazard or risk analyses *per se*".

B.4 ISO/CEN classification of health software products

ISO and CEN, through their health informatics technical committees ISO/TC 215 and CEN/TC 251, have published identical Technical Specifications on classification of safety risks from health software, see Bibliography [11] [12]. These Technical Specifications provide the means for broad screening of health software products so as to classify them according to the risk they might present to patients. One anticipated application of the classification is as a precursor to assigning design and production controls appropriate to risk.

The Technical Specifications propose five "risk classes" based on the "consequences" to a patient if a health software product were "to malfunction or be the cause of an adverse event" and the "likelihood" that the "consequence" would be realised in "reasonably foreseeable circumstances".

Consequences are categorized as:

- catastrophic;
- major;
- considerable;
- significant;
- minor.

The meaning of these categories is tabulated in Table B.1.

Table B.1

Category	Interpretation	
	Consequence	**Number of patients affected**
Catastrophic	Deaths	Multiple
	Permanent life-changing incapacity and any condition for which the prognosis is death or permanent life-changing incapacity; severe injury or severe incapacity from which recovery is not expected in the short term.	Multiple
Major	Death	Single
	Permanent life-changing incapacity and any condition for which the prognosis is death or permanent life-changing incapacity; severe injury or severe incapacity from which recovery is not expected in the short term.	Single
	Severe injury or severe incapacity from which recovery is expected in the short term.	Multiple
	Severe psychological trauma	Multiple
Considerable	Severe injury or severe incapacity from which recovery is expected in the short term.	Single
	Severe psychological trauma	Single
	Minor injury or injuries from which recovery is not expected in the short term.	Multiple
	Significant psychological trauma	Multiple
Significant	Minor injury or injuries from which recovery is not expected in the short term.	Single
	Significant psychological trauma	Single
	Minor injury from which recovery is expected in the short term.	Multiple
	Minor psychological upset; inconvenience	Multiple
Minor	Minor injury from which recovery is expected in the short term; minor psychological upset; inconvenience; any negligible consequence.	Single

The likelihood of a consequence being realised in practice are categorized as:

- very high;
- high;
- medium;
- low;
- very low.

The categories are to be interpreted as:

Likelihood	Scope
Very high	Certain or almost certain; highly likely to occur
High	Not certain but very possible; reasonably expected to occur in the majority of cases
Medium	Possible; not unlikely to occur
Low	Could occur but in the great majority of occasions will not
Very low	Negligible or nearly negligible possibility of occurring

Finally the “risk class” into which a product falls is determined by the following matrix.

Likelihood	Consequence				
	Catastrophic	Major	Considerable	Significant	Minor
Very high	A	A	B	B	C
High	A	B	B	C	C
Medium	B	B	C	D	D
Low	B	C	D	D	E
Very low	C	C	D	E	E

Class A represents the highest potential risk and Class E the lowest.

Of significance is the following requirement.

“In identifying the hazards which a health software product or product type may present to a patient, a hazard shall not be dismissed simply because it is believed that the design of the product is such that there are no circumstances in which the hazard would arise because of the particular product or general design features. The potential for harm (hazards) that the product could present shall be determined as if such design features and controls were not present or malfunctioned.

In identifying the hazards which a health software product may present to a patient, if it were to malfunction or be the cause of an unintended event shall also not be dismissed simply because, even if the hazard were to arise, no adverse consequences to a patient would occur because, for example, of vigilance of the user or other events external to the product. This aspect is addressed by the assignment of likelihood to the consequence occurring.”

Also the following:

“In assessing likelihood, the likelihood of a consequence shall not be diminished in relation to any feature of the product itself (including associated instructions for use). Likelihood in the context of this section is not the likelihood of the product malfunctioning or being responsible for an adverse event. It is the likelihood of the consequences of that malfunction or adverse event actually being realized in practice.

However it is permissible to take account of reasonably foreseeable circumstances external to the product. Thus if, for example, the identified consequence of a hazardous event could be injury, the likelihood of that consequence resulting in actual injury to a patient may take account of matters such as the possibility:

- of the hazardous event being noticed by a user with appropriate qualifications before the consequence occurs;
- of the consequence being avoided because the number of events over a period of time which would take place before the consequence would result, would enhance the possibility of the hazard being identified;
- that a patient would be seen by a healthcare professional before any harm occurred and in sufficient time for effective treatment or therapy to be delivered.”

The Technical Specifications provide advice on how to apply these requirements to health software products.

The Technical Specifications' approach to classifying health software products is consistent with the FDA approach to classifying “software in medical devices” (Bibliography [9]) and “off-the-shelf software” (Bibliography [10]) (see B.3).

The three FDA “levels of concern” could readily be aligned with the Technical Specifications' five “consequence” categories. However, the FDA “level of concern” is not explicit in respect to likelihood of a consequence, e.g. death or injury, actually occurring in practice. It also applies to the safety of the “operator” as well as to patients rather than solely to the patient *per se*.

B.5 Conclusions

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” and “off-the-shelf” 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.

Annex C
(informative)

Risk management

C.1 General

If risk management is to be a control measure then there will be a need for underpinning standards. This annex considers the suitability of standards that are currently available.

NOTE This review is only for the purpose of this document and seeks to highlight and summarise only those aspects of significance to this document. It should not be used as a definitive guide in any respect or for any purpose (the original documentation and the competent national authorities should be referred to).

C.2 Attributes necessary for successful uptake of risk management processes

For risk management to be successfully applied to health software products, key attributes need to exist within the standard(s), guidance and tool(s) adopted. These are:

— a simple-to-understand underlying process, including logic of calculated results, not mandating the use of external personnel and other specialists;

— capture of all the key components of risk;

— capacity to measure and weigh elements in a healthcare language and in a context of far-from-complete historic event and incident data that would allow a quantitative approach;

— flexibility in terms of analysis detail and controls recommendations, commensurate with the complexity of the health software product, the calculated levels of risk and the stage of the product's development;

— the ability to iterate and expand the risk assessment and management capabilities as the development of the health software product proceeds;

— support for the component processes, and the complex nature of health software products, in the form of knowledge bases, to support use by the "non-expert".

These attributes have been used to evaluate the various candidate standards.

C.3 Minimum components for an effective risk management process

Many areas complementary to health software product development, such as information security, have adopted risk management processes with considerable effect. Whilst these are considered in C.6, the identified components of general risk management good practice, also provide useful indicators of an acceptable process for health software product development:

— identification of the health software product's component assets and the threats to, and vulnerabilities of, those assets;

— impact assessment (to the producer, user and patient recipient of the health software product);

— threat likelihood and vulnerability assessment;

- determination of risk levels (as a compound outcome of impact, threat and vulnerability levels);
- identification of recommended (i.e. justified and appropriate) controls;
- comparison with existing controls, to identify areas of remedial risk;
- options for risk treatment, including direct management, risk acceptance, avoidance, managed transference, etc.;
- risk treatment planning (i.e. of control implementation).

C.4 “Enterprise risk management” processes

C.4.1 General

“Enterprise risk management” is an emerging term that is being used to place greater emphasis on the holistic nature of the process and thus its applicability across the totality of an organization and its operations.

As such these standards can be expected to be high level documents, laying out a general framework rather than a detailed process model with the associated expertise/knowledge bases to support risk analysis and risk management of health software products.

C.4.2 PD 6668:2000 — “Managing risk for corporate governance”

The “published document” PD 6668:2000 [58] essentially forms a management primer on risk management and covers:

- a background to the drivers for risk management;
- an outline of the broader considerations of corporate governance;
- a description of a framework for risk management;
- a practical guide to delivering business requirements for strategic risk management;
- a benchmarking questionnaire for organizations' risk management frameworks.

The framework encompasses:

- the classic, management systems approach of plan, do, check and act (PDCA);
- risk management activity at three levels (strategic, management, operational);
- threat identification;
- risk assessment;
- deciding on how risks are to be managed;
- identifying resources;
- planning the management of individual risks;
- communications;
- monitoring and measuring.

However, the process model is only given in outline although the concept of “likelihoods” is explicitly acknowledged. In contrast, there is confusion between threats and countermeasures, e.g. “(failure to establish) effective contingency arrangements” is quoted as an example of the former rather than as an example of the latter.

Furthermore, the matrices used are all predicated on “low”, “medium” and “high” type assessments, that do not therefore lend themselves to any more than 3 classes/measures of risk and thus would deliver insufficiently customized frameworks of controls.

Finally, and of fundamental importance to this Technical Report, the guidance document gives almost no guidance on countermeasures, and the lists of other components, such as threats, are provided “as examples only”. As a high level document, therefore, it is not sufficiently comprehensive nor customized to the healthcare sector to provide a mechanism for ensuring patient safety in respect of health software products.

C.4.3 Australia and New Zealand — AS/NZS 4360:2004

The Australia and New Zealand standard AS/NZS 4360:2004 [59] has been adopted, at national level, by a variety of healthcare organizations for the purposes of corporate governance, including the UK National Health Service. Concepts within it, such as that of “risk treatment”, have also been taken up in other risk-based standards, such as BS 7799-2:2002 (see C.6.1). It is another high level description of the required process albeit with an associated risk management guidelines document. The latter is more of a compendium of possible processes rather than a recommended approach.

It sets out a classic/generic “process” for management of risk, independent of a particular industry or economic sector, whilst accepting the need for flexibility in implementation.

It notes that the establishment of probability of occurrence and the possible consequences needs to be, and can be, qualitative, semi-qualitative or quantitative depending on whether incident statistics exist. However, it expands on this with a list of pertinent information sources and techniques that can be employed. The guidelines provide more guidance on:

- the choice of analysis method (that will need to be sensitive to the situation);
- workable consequence and likelihood scales;
- the types of risk measurement scales that can be applied;
- different techniques for the meaningful expression of risk levels.

In the area of risk treatment, AS/NZS 4360 again provides significant details on options for the treatment of risks with negative outcomes (i.e. as is the case with patient safety risks), with the content addressing:

- avoiding the risk by deciding not to start or continue with an activity;
- adoption of measures that will change the likelihood of negative outcomes;
- adoption of measures that will change the consequences to reduce the extent of losses – such as insurance and contingency planning;
- sharing of risk via contracts, etc., to transfer liability;
- retention/acceptance of risk.

Furthermore, and crucially, it also sets out guidance on designing risk treatment plans that suitably trade off treatment costs versus benefits to allow objective risk acceptance. In contrast and conflict with this however, it also focuses strongly upon reducing risk to a level as low as reasonably practical (ALARP). Practice too often shows this principle is then adulterated into an unsustainable and inappropriate “risk avoidance” mentality.

As a generic guide, it can be appreciated that this standard is well developed. However, its incomplete expertise content and lack of healthcare informatics product specifics makes it unsuitable, as it stands, for the purposes of this Technical Report.

C.4.4 ISO/IEC WG on risk management

The ISO/IEC (Technical Management Board's) Joint Working Group on Risk Management [35] was formed in the middle of 2005. The working group's intention is to create an International Standard based upon enhancements to an existing national standard where needed. A working draft has been published for comment. This draft is intended to be:

"a top-level, generic, guidance document" that "...provides support to existing standards for specific risk applications…" and "...delivers concepts and frameworks that are independent of legislative and regulatory constraints." but which are "…applied with minimal modification…" as "…a focus of everyday business practice…".

The document has been structured around:

- a set of principles of good risk management practice;
- an organizational context for risk management;
- a risk management framework, made up of:
  - communication and consultation;
  - establishing the (business) context;
  - risk identification;
  - risk evaluation;
  - risk treatment;
  - monitoring and review.

Differently to its peer standards, this framework includes the evaluation of existing controls as part of the risk analysis, thereby not identifying the "underlying" risk and placing the focus on the "net risk". It's reasoning for doing so is unclear. The draft is written primarily in terms of risks to an organization, rather than the application of risk analysis and risk management to the safety of a product. Thus, it would be inadequate for the latter in the context of ensuring the safety of health software products.

As with the other "high level" standards, this working draft contains lists of examples but does not offer a definitively specified process with supporting expertise.

C.4.5 Conclusions regarding "enterprise" risk management standards

Not being targeted at healthcare, none of the standards reviewed in this section provides a sufficiently clear or definitive process model for adoption for the purposes of this Technical Report. However, there is a general level of commonality between their proposed processes. Various components from each of the documents, especially those of AS/NZS 4360, would be candidates for adoption for health software products.

C.5 "Healthcare related" risk management standards

C.5.1 ISO 14971:2007 — Application of risk management to medical devices

ISO 14971:2007 [36] is the recognised International Standard for the application of risk management to medical devices. The medical devices quality system standard, ISO 13485:2003 [27] refers specifically to ISO 14971 for risk management. The (FDA) also recognised ISO 14971 in 2001 as the primary risk management standard for medical devices.

The final report of the World Standards Cooperation's (WSC) Healthcare Technology Task Force (HTTF) [60] January 2006 (recommendation 4):

"noted the recent efforts by the ISO Technical Management Board (TMB) task force to develop a more global risk management standard. WSC should ensure that development of a more general risk management standard does not pre-empt, change, or interfere with the existing ISO 14971, an International Standard commonly in use by the medical device community."

ISO 14971 presents an overview of the risk management process that is intended to be used as part of a quality system. Conformance to the International Standard requires the following actions:

- establish a risk management process;
- establish a policy on acceptable risk;
- hire and train qualified personnel;
- risk analysis;
- risk evaluation;
- risk control;
- conduct of a final risk benefit analysis and provision of information on residual risk;
- post production information.

The following risk analysis techniques are included in ISO 14971:2007:

- Failure Mode and Effect Analysis (FMEA);
- Fault Tree Analysis (FTA);
- Hazard and Operability Study (HAZOP).

No impact assessment tools or techniques are provided and that International Standard blurs together the concepts of impact assessment, threat and vulnerability assessment and controls. Furthermore, it suggests that the process of making decisions on the acceptability of the identified risks, while taking into account the mitigations implemented in the design process, is a risk evaluation activity. This is contrary to the consensus of the other standards reviewed in this Technical Report. A useful risk controls table is, however, included.

C.5.2 GHTF/SG3/NI5R8 — Risk management principles and quality management systems

GHTF/SG3/NI5R8 [39] looks at the implementation of risk management principles and activities within a quality management system. It asserts that medical device manufacturers are generally required (e.g. by regulatory or legislative requirements) to have a quality management system in place as well as processes for addressing device-related risks.

Whilst the processes for managing risk can evolve into a stand-alone management system, medical device manufacturers are recommended to integrate them to reduce costs, eliminate redundancies, and lead to a more effective management system. The document is intended to assist medical device manufacturers with the integration of a risk management system or risk management principles and activities, into their existing quality management system. It does this by way of worked examples.

Annex A of ISO 15941:2007 depicts a matrix of severity of harm versus probability of occurrence (more accurately likelihood) although the results are suggested as simply “low, medium and high” with red, amber and green colours assigned to the intersection cells. It also provides a useful, but high level, depiction of a flow process for risk management within design and development. The importance of considering and agreeing upon the level of risk that is acceptable is also emphasised as an early step in the process.

However it does not address the risk management principles within its title in any detail and it is unlikely that the document would be immediately usable by other than an expert.

C.5.3 ISO/IEC 62304 — Medical device software lifecycle processes

ISO/IEC 62304 [61] has been prepared by a joint ISO/IEC working group, made up of members of Subcommittee 62A: *Common aspects of electrical equipment used in medical practice*, of IEC technical committee 62: *Electrical equipment in medical practice*, and finally members of ISO Technical Committee 210, *Quality Management and Corresponding General Aspects for Medical Devices*.

It combines the requirements for a software life cycle model, as described in ISO 12207:1995 [30] and its Amendment [31], with a risk based approach according to ISO 14971 [36]. ISO 12207 applies to the development and maintenance of medical device software when software is itself a medical device or when software is an embedded or integral part of the final medical device. That International Standard does not cover validation and final release of the medical device, even when the medical device consists entirely of software.

It provides a framework of processes, activities and tasks necessary for the safe design and maintenance of medical devices. That International Standard covers controls only in outline.

C.5.4 FDA — Design control guidance for medical device manufacturers

The FDA document, Design Control Guidance for Medical Device Manufacturers [34] is written to provide assistance to device manufacturers in understanding quality system design control requirements and applies to the design of medical devices as well as the design of the associated manufacturing processes. The guidance discusses subjects in the order in which they appear in the FDA Quality System regulation that is unlikely to be suited (directly) to all other users. It provides a definition of what design controls are and why they are important. However, whilst reference is made that risk management is a process that is to be integrated across the whole design process, only limited guidance is provided on its content within the sections.

C.5.5 Australia and Canada

The Australian, Medical Device Guidelines — Conformity Assessment Procedures [62] and the Canadian Medical Device COMPLIANCE and Enforcement Directive [63] both deal with conformity assessment procedures but neither provides structured discussion of risk management other than by implications.

C.5.6 Conclusions regarding health related risk management standards

The healthcare related standards above routinely use phrases and terms such as “risk analysis”, “risk assessment” and “risk management”. Most use the terms to reference the classification that a medical device has been given. However, as has been shown, these classes (whilst they may be the result of a historic formal assessment) essentially relate to the safety impact that could occur and the levels of threat and vulnerability (i.e. combined as likelihood) have not been considered adequately, if at all. Indeed, most of these standards and guidance documents have made extensive use of phrases such as “for example” and “including”, such that they also do not provide a process that can just be adopted. Instead, some considerable assembly of knowledge is required to make them effective.

In contrast, the guidance and standards documents do contain enough content to strongly suggest that medical devices and health software products are not synonymous.

Furthermore, whilst many of the suggested controls for medical devices would be applicable to health software products, the nature of these products may require different controls to be applied. Some of the controls in the above standards are mandated more by legislative objectives than by the defined/identified risk and this Technical Report makes no assumption about legislative measures.

In developing a standard for ensuring patient safety of health software products, ISO 14971 and GHTF/SG3/NI5R8 will be the most relevant, although useful components can be obtained from most of the documents reviewed.

Taken together, the above standards and guidelines deliver a useful reminder of the need for risk analysis and management to cover both the “design and develop” process and, critically, to operate as a basis of “monitoring and maintaining compliance”, i.e. as a “lifecycle” process. This is especially important as health software products are typically more regularly re-released in new, subtly changed, versions rather than medical devices which are more often substituted by materially new products.

C.6 Related risk management standards

C.6.1 BS 7799-2:2002/ISO/IEC 17799:2005/ISO/IEC 27001:2005

The range of documents BS 7799-2:2002/ISO/IEC 17799:2005 [65]/ISO/IEC 27001:2005 [64] addresses best practices in the field of information security management, i.e. the domain within which any health software product will be operated. BS 7799 was originally developed in 1995 and has since been regularly updated and increasingly “internationalized”. Inasmuch as its definition of information security covers confidentiality, integrity and availability, it can be said to already address many of the aspects of safety criticality, especially when patient safety is employed as a qualitative impact valuation topic.

The British Standard was made up of two parts.

- Part 1 provides a set of commonly applicable control objectives arranged into sub-groups and major objectives.

- Part 2 defines the concept of an Information Security Management (Lifecycle) System, consistent with those in respect of safety criticality, quality, IT operations and environmental protection. The information security management system is similarly predicated upon the plan, do, check and act (PDCA) model.

The control objectives are very relevant to, and could be easily translated into, patient safety risk assessment concerns. They cover:

- security policy;

- organization and management of security;

- asset classification and control;

- personnel security;

- physical and environmental security;

- communications and operations management;

- access control;

- systems development and maintenance;

- business continuity management;
- compliance;
- incident management.

BS 7799-2 has been internationally adopted as ISO/IEC 27001, with the content aligned to what had previously been ISO/IEC 17799:2005. BS 7799-1 had already been internationalized as ISO/IEC 17799:2005 but is expected to evolve into ISO 27002 in due course. Additionally, a range of other products are expected to be produced in this series in the near future.

Of relevance to this Technical Report is the standard's central dependence upon a highly structured and suitably comprehensive (and detailed) risk assessment of the business processes, IT services and infrastructures (hardware, software, media, documentation, etc.) employed within the scope of the information security management system.

In addition to legal and regulatory requirements, ISO/IEC 27001:2005 4.2.1 b) now also places extra emphasis on the consideration of contractual obligations at all stages of the information security management system, especially in respect of risk assessment, risk treatment, the selection of controls, the control of records and resources, the monitoring and reviewing of the information security management system and in the documentation requirements.

Furthermore, an additional document, BS 7799-3:2006 [69], on ISMS risk management, will be adopted in the future as ISO/IEC 27005 [66]. It provides similar information to that provided in the BSI's Published Document PD 3002:2000. The latter document provided a comprehensive description of the challenges in performing information security risk management effectively, in a very similar form to the list of key components in C.3.

The ISO 2700X series of International Standards clearly points in the same general direction as IEC 61508-3 and -5 (see C.6.2). However, it again does not offer comprehensive specifications of the processes or topics to be covered. In contrast, the scope of ISO 27001 would be highly reusable in respect of patient safety risk assessments of health software products.

C.6.2 IEC 61508 — Safety critical risk assessment

IEC 61508 is made up of a set of eight components, with a part 0 forming an overview. The core of the components (parts 1 to 4) were drafted in 1998 with section 2 (requirements for safety-related systems) being re-drafted in 2000. All four parts are currently the subject of a committee draft ballot of revisions issued in December 2005. Parts 5, 6 and 7 will then follow.

The standard applies to electrical, electronic and programmable electronic systems. At one time, it was questioned whether IEC 61508 was limited to programmable logic controllers but recent work has, for example, encompassed IT network-based safety-related systems with connections to the internet, thereby underscoring the standard's applicability to all programmable systems and irrespective of their particular application.

IEC 61508 is intended to be operated in conjunction with ISO 9000, and is predicated on the basis that:

- absolute safety (zero risk) cannot be obtained;
- systems pose risks that must be understood;
- risks that are intolerable must be reduced or avoided;
- confidence of safety must be derived in advance, not retrospectively, through design;
- safety must be demonstrable;
- dispelling the belief that "done (i.e. built) well it will automatically be safe" is critical;
- correct functionality does not necessarily equal safety.

The sections of IEC 61508 that are relevant to this technical report are:

- Part 1: General Requirements;
- Part 3: Software Requirements (i.e. for software components);
- Part 5: Examples of methods for the derivation of safety integrity levels.

To use the standard effectively undoubtedly requires a good understanding of risk management and the current revision of parts 1 to 4 are in part a response to a body of opinion which asserts that the defined processes are both too complex and too ambiguous.

At the heart of the standard is the concept of “safety integrity levels” (SILs), that are somewhat analogous to risk levels. Although specific processes for the allocation of SILs are not provided, Part 5 provides a range of alternative methods. Principal amongst these is risk classification based on a mapping of frequency and consequence from which one of four risk classes is derived. With frequency being clearly synonymous with “likelihood”, this is a true risk-based process and comes to the same conclusions as GHTF/SG3/NI5R8 [39].

However, Part 5 of the standard's examples remain at a high level and do not extend down to comprehensive lists of criteria to be considered or controls that are suitable for being adopted. Also of concern is the standard’s relative preference for quantitatively generated risk measures, although the potential role for qualitative assessment is also recognised. Certainly the former will be almost impossible to apply where there is no reliable or extensive bank of statistics upon which to draw.

Whilst ICE 61508 represents a set of concepts and principles which could be considered for the risk assessment of patient safety relating to health software, the mechanisms within the standard as currently defined are generally recognised as complex and difficult to implement in a sustainable manner. Therefore, whereby any future risk assessment process for health software might apply the essential principles, it is not considered suitable. Additionally it will be particularly important to achieve general consistency with the medical devices arena where ISO 14971 is already used (see C.5.1) and which applies different, generally more practical, mechanisms.

C.6.3 CRAMM — UK Government's information security risk method

CRAMM [40] is a commercially-available method. Exceptionally it has been reviewed in this document in recognition of its intellectual property right being held by UK Government, its extensive and successful adoption by many health care organizations and its application throughout the UK National Health Service.

The method has been established some 17 years and has been the subject of regular review and maintenance. For almost all of that time it has been supported by a semi-automated tool and it is understood that more 600 copies of the tool have been deployed in more than 25 countries.

The method and its automation tool supports:

- the BS 7799/ISO 27001 information security management process;
- asset and dependency modelling;
- information security risk analysis and management, including risk treatment;
- specification of continuity and recovery requirements;
- creation of a library of re-usable risk and compliance models;
- iterative assessments using “express” and “expert” functionality levels that interoperate;
- risk and compliance report production;
- security improvement business cases and implementation planning.

Information security is understood to be considered by CRAMM as in ISO 27001 and CRAMM contains knowledge bases/expertise covering:

- nearly 400 types of asset (covering types of business processing, IT services, hardware, software, communications protocols, media and locations);
- 26 different types of impact (covering confidentiality, integrity and availability issues);
- impact valuation on 10-point quantitative and/or qualitative scales;
- some 40 types of threat and vulnerability (covering accidental, deliberate, technical and human types, etc.) as well as the questions it is necessary to answer in order to evaluate these;
- seven levels of risk;
- eight information security domains (hardware, software, communications, personnel, documentation, procedural, physical and emissions);
- nearly 3 500 countermeasures (organized into hierarchical groupings of increasing detail covering policy statements, objectives, functions and working examples) indexed back to the threats and assets for which they are an appropriate response.

From the above, it is clear that an approach akin to, or built upon, CRAMM could quite effectively address the assessment of the patient safety of health software products, by codifying the present expertise, making the information and processes generally available and by simplifying their execution by non-experts.

C.6.4 Conclusions regarding related risk management standards

All of the standards described in this Clause clearly have a close relevance to ensuring the patient safety of health software products, although none does so in any immediately usable form.

Taken together, ISO 27001 and CRAMM provide almost a worked example of what could be achieved using a method and tool that was also compliant with IEC 61508 concepts.

C.7 Overall conclusions regarding risk management standards

This review shows that there are numerous risk management documents and standards and tools available, with many of them addressing legislative and regulatory requirements (that are not a “given” for this Technical Report) or medical devices (which are clearly different in nature). Of the latter, some of those standards include, within their scope, software products, albeit as effective appendages of the medical devices themselves.

This review of standards has shown that they are either too generic or too complex for ready application to the purposes of this Technical Report, i.e. the particular challenges of patient safety in respect of health software products, by “non-expert” personnel (with any confidence of surety of the accuracy of outcomes).

Whereas clearer guidance will be available when the ISO/IEC JWG standard (Bibliography [35]) is finalised, it is clear that there is already considerable commonality and consensus around the key components of an effective risk management process.

Many components of the standards reviewed, especially the lists of examples, would be very usable, if combined. However, such combination would still not provide exhaustive lists and further work would be required.

Nevertheless, in developing any standard for ensuring the patient safety of health software products, all of the documents reviewed above have some contribution to make.

Based on the range of documents reviewed and their pragmatic use of high level descriptions and lists of examples, it is highly unlikely that a single document could be expected to encompass all of the concepts and expertise required to ensure the patient safety of health software products. Even if that were to be achieved, it is highly improbable that the document would also be capable of effective use “in the field” without the provision of a support tool or tools.

Taken together, ISO 27001 and CRAMM provide almost a worked example of what could be achieved.

The overall conclusions are that, 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 the ISO/IEC JWG, ISO 14971 and IEC 61508, is required specifically for health software products; that standard should embody the concepts in GHTF/SG3/NI5R8 and build on the experience of the use of CRAMM with ISO/IEC 17799;

- the new standard should be backed by an implementation guide specific to health software products.

Bibliography

[1] KOHN, I.T., CORRIGAN, J.M. and DONALDSON, M.S., *To Err is Human: Building a Safer Health System*, USA Institute of Medicine, National Academy Press, 1999

[2] *An Organisation with a Memory*, HMSO, June 2000

[3] *Quality in Australian Healthcare*, Study, 1994

[4] BRENNAN, T.A., LEAPE, I.I., LAIRD, N.M., HERBERT, I., LOCALIO, A.R. and LAWTHERS, A.G., *Incidents of adverse events and negligence in hospitalised patients*, results of the Harvard Medical Practice Study, New England J Med., **324**, 1991, pp 370-376

[5] *Quality of care: patient safety*, Report of the WHO Secretariat, EB 109/9, 5 December 2001

[6] *Building a safer NHS for Patients*, UK Department of Health, April 2001

[7] ISO/IEC Guide 51:1999, *Safety aspects — Guidelines for their inclusion in standards*

[8] Information document concerning the definition of the term "Medical Device", Final document GHTF/SG1/N29R16:2005, GHTF Study Group 1, the Global Harmonization Task Force, 29 June 1999

[9] *Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices*, Center for Devices and Radiological Health, Food and Drug Administration, US Department of Health and Services, 11 May 2005

[10] *Off-the-Shelf Software Use in Medical Devices, Guidance*, Center for Devices and Radiological Health, Food and Drug Administration, US Department of Health and Services, 9 September 1999

[11] ISO/TS 25238, *Health informatics — Classification of safety risks from health software*

[12] CEN/TS 15260:2006, *Health informatics — Classification of safety risks from health informatics products*

[13] EN 1041:1998, *Information supplied by the manufacturer with medical devices*

[14] ISO 14155 (both parts), *Clinical investigation of medical devices for human subjects*

[15] ISO/TS 19218:2005, *Medical devices — Coding structure for adverse event type and cause*

[16] *Adverse Event Reporting Guidance for the Medical Device Manufacturer or its Authorized Representative*, Final Document GHTF/FD:99-7, GHTF Study Group 2, the Global Harmonization Task Force, 29 June, 1999

[17] UK National Patient Safety Agency, http://www.npsa.nhs.uk

[18] ISO/TS 22224, *Health informatics — Electronic Reporting of adverse drug reactions*

[19] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices

[20] Guide to the implementation of directives based on the New Approach and the Global Approach, European Commission, Luxembourg, Office for Official Publications of the European Communities, 2000, ISBN 92-828-7500-8

[21] http://europa.eu.int/comm/enterprise/medical_devices/meddev/index.htm

[22] *Guidance on Quality Systems for the Design and Manufacture of Medical Devices*, GHTF.SG3.N99-8, Global Harmonization Task Force, 29 June 1999

[23] ISO 9001:1994: *Quality systems — Model for quality assurance in design, development, production, installation and servicing*

[24] ISO/TR 14969:2004, *Medical devices — Quality management systems — Guidance on the application of ISO 13485:2003*

[25] Quality System Regulations, 21 CFR Part 820 (Federal Register, October 7 1996, Part VII 21 CFR Parts 808, 812 and 820 Medical Devices; Current Good Manufacturing Practice (CGMP); Final Rule)

[26] Medical Device Quality Systems Manual: *A Small Entity Compliance Guide*, Center for Devices and Radiological Health, FDA, December 1996

[27] ISO 13485:2003, *Medical devices — Quality management systems — Requirements for regulatory purposes*

[28] ISO 9001:2000, *Quality management systems — Requirements*

[29] ISO/IEC 90003:2004, *Software engineering — Guidelines for the application of ISO 9001:2000 to computer software*

[30] ISO/IEC 12207:1995, *Information technology — Software life cycle processes*

[31] ISO/IEC 12207:1995/Amd.1:2002, *Information technology — Software life cycle processes Amendment 1*

[32] ISO/IEC TR 15271:1998, *Information technology — Guide for ISO/IEC 12207 (Software Life Cycle Processes)*

[33] *Design Control Guidance for Medical Device Manufacturers*, GHTF.SG3.N99-9, Global Harmonization Task Force, 29 June 1999

[34] *Design Control Guidance for Medical Device Manufacturers*, Center for Devices and Radiological Health, FDA, 11 March 1997

[35] ISO 31000, *General guidelines for principles and implementation of risk management*

[36] ISO 14971:2007, *Medical devices — Application of risk management to medical devices*

[37] IEC 61508-3:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software Requirements*

[38] IEC 61508-5:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels*

[39] GHTF/SG3/NI5R8, Global Harmonization Task Force Study Group 3, Risk Management Principles and Quality Management Systems, May 2005

[40] CRAMM, UK Government’s Preferred Risk Analysis and Management Method for Information Security Management, January 2003

[41] Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices

[42] Council Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on *in-vitro* diagnostic medical devices

[43] Therapeutic Goods Act 1989 as amended by the Therapeutic Goods Amendment (Medical Devices) Bill 2002 and the Therapeutic Goods (Medical Devices) Regulations 2002 [known as Therapeutic Goods Amendment (Medical Devices) Act 2002]

[44] Australian Medical Devices Guidelines: *An Overview of the New Medical Devices Regulatory System*, Guidance Document Number 1, Version 1.6, Therapeutic Goods Administration, Department of Health and Ageing, 23 May 2003

[45] Differences between the Australian and European Union regulatory systems (1), *Fundamental differences and classification*, Fact Sheet, Draft for comment, Therapeutic Goods Administration, Australian Department of Health and Ageing, December 2004

[46] Differences between the Australian and European Union regulatory systems (2), *Essential principles*, Fact Sheet, Draft for comment, Therapeutic Goods Administration, Australian Department of Health and Ageing, April 2005

[47] Medical Devices Regulations 1998 of the Food and Drugs Act

[48] *Medical Device Compliance and Enforcement Directive*, Health Products and Food Branch Inspectorate, Health Canada, 11 February 2004

[49] *Guidance for the Risk-based Classification System*, Draft, GD006, Therapeutic Products Directorate, Medical Devices Bureau, Health Canada, 4 May 1998

[50] *Guidance for the Risk-based Classification System of In Vitro Diagnostic Devices*, Draft, GD007, Therapeutic Products Directorate, Medical Devices Bureau, Health Canada, 17 March 1998

[51] *Keyword Index To Assist Manufactures In Verifying The Class of Medical Devices*, Therapeutic Products Programme, Licensing Services Division, Medical Devices Bureau, Health Canada

[52] *Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices*, Center for Devices and Radiological Health, Food and Drug Administration, US Department of Health and Human Sciences, 11 May 2005

[53] *Off-The-Shelf Software Use in Medical Devices*, Center for Devices and Radiological Health, Food and Drug Administration, US Department of Health and Human Sciences, 9 September 1999

[54] *General Principles of Software Validation*; Final Guidance for Industry and FDA staff, Center for Devices and Radiological Health, Food and Drug Administration, US Department of Health and Human Sciences, 11 January 2002

[55] *Principles of Medical Devices Classification*, Proposed Document SG1/N015R22, GHTF Study Group 1, the Global Harmonization Task Force, 17 November 2003

[56] *The Classification Rules*, Bulletin Number 10, UK Medical Devices Agency (now UK Medicines and Healthcare products Regulatory Agency), February 1995

[57] *Classification of Medical Devices*, Guidance Document Number 25, Therapeutic Goods Administration, Australian Department of Health and Ageing, January 2005

[58] PD 6668, *Managing Risk for Corporate Governance*, British Standards Institution, November 2000

[59] AS/NZS 4360:2004, *Risk Management*, Standards Australia Institute

[60] World Standards Cooperation Healthcare Technology Task Force (HTTF), Final Report, January 2006

[61] IEC 62304:2004, *Medical device software — Software life cycle processes*

[62] Australian Medical Devices Guidelines — *Conformity Assessment Procedures*, Guidance Document Number 3, Version 1.5, Therapeutic Goods Administration, Australia, 23rd May 2003

[63] Medical Device Compliance and Enforcement Directive, Health Canada, 11th February 2004

[64] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

[65] ISO/IEC 17799, *Information technology — Security techniques — Code of practice for information security management*

[66] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[67] IEC 60601-1-4, *Medical electrical equipment — Part 1-4: General requirements for safety — Collateral Standard: Programmable electrical medical systems*

[68] EN 1441, *Medical devices — Risk analysis*

[69] BS 7799-3, *Information security management systems — Guidelines for information security risk management*

ICS 35.240.80

Price based on 38 pages