TECHNICAL SPECIFICATION

ISO/TS 25238

First edition
2007-06-15

Health informatics — Classification of safety risks from health software

Informatique de santé — Classification des risques de sécurité à partir d'un logiciel de santé

Reference number
ISO/TS 25238:2007(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.

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

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

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order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn.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

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

ISO/TS 25238 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Introduction

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

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

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

It is increasingly claimed that information systems such as decision support, protocols, guidelines and pathways could markedly reduce such adverse effects. If only for this reason (quite apart from others, which do exist), this is leading to increasing utilization of decision support and disease management systems, which will inevitably 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 criticized 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 the cost of clinical investigative tests is another.

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

— poor evidence base for design;

— failure in design logic to properly represent design intentions;

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

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

— failure to update in line with current knowledge.

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

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

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

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

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

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

Failures and deficiencies in health software products can, of course, have adverse impacts other than by 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 Technical Specification 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 Technical Specification 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 Technical Specification.

The safety of medicines and of medical devices is assured in many countries through a variety of legal and administrative measures, e.g. in the European Union it is subject to several EU directives (see References [7], [8] and [9]). 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 European Committee for Standardization (CEN) and the International Electrotechnical Commission (IEC). Software necessary for the proper application or functioning of a medical device is often encompassed by these legislative controls. However, other software applied to health is not usually covered in this way. This Technical Specification is concerned with software applied to health excluding that which is necessary for the proper application or functioning of a medical device.

A necessary precursor for determining and implementing appropriate design and production controls, in order to minimize risks to patients from product malfunction or inadequate performance, is a clear understanding of the hazards that 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 manufacturers of health software products on design and production control (and corresponding standards produced), then it will need to be recognized 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 that 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 together products in a limited number of classes or types according to the risk they might present.

This Technical Specification presents a process for such a grouping of health software products. It proposes five risk classes and will facilitate broad screening of generic product types and of individual products to allow different levels of, or rigour in, the application of design and production controls that are matched to risk. Thus, the classification proposed may be a precursor for standards on design and production control, where the latter might require a far more detailed, in-depth and rigorous risk analysis for a particular product than that required for the broad classification process in this Technical Specification. Examples of the application of the process for assigning a risk class are given for a number of different types of health software products.

The term “health software products” refers to any health software product, whether or not it is placed on the market and whether it is for sale or free of charge. This Technical Specification therefore covers commercial products as well as, for example, open-source health software and software created for, and used in, only one health organization, such as a hospital. There is a broad range of health software products, ranging from simple research databases to call and recall systems, clinical decision support, electronic health record systems, ambulance dispatch systems, hospital clinical laboratory systems and GP systems. Annex B provides four examples of the application of this Technical Specification to different health software products. However, any software that is necessary for the proper application or functioning of a medical device is outside the scope of this Technical Specification.

Health informatics — Classification of safety risks from health software

1 Scope

This Technical Specification is concerned with the safety of patients and gives guidance on the analysis and categorization of hazards and risks to patients from health software products, in order to allow any product to be assigned to one of five risk classes. It applies to hazards and risks which could cause harm to a patient. Other risks, such as financial or organizational risks, are outside the scope of this Technical Specification unless they have the potential to harm a patient.

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

This Technical Specification does not apply to any software which is necessary for the proper application or functioning of a medical device.

NOTE This Technical Specification is intended for the assignment of health software to broad risk classes, so as to aid decisions such as what controls should be applied to ensure safety. It is not intended for the application of risk analysis and risk management to the design of health software products and the mitigation of any identified risks to acceptable levels (see Annex A).

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 the health or well-being of a patient

[adapted from ISO/IEC Guide 51:1999]

2.2
hazard
potential source of harm

[ISO/IEC Guide 51:1999]

2.3
health software product
software proffered for use in the health sector for health-related purposes, but excluding software necessary for the proper application of a medical device

2.4
manufacturer
natural or legal person with responsibility for the design, manufacture, packaging or labelling of a health informatics product, assembly of a system or adaptation of a health informatics product before it is placed on the market and/or put into service, regardless of whether these operations are carried out by that person or on that person's behalf by a third party

[adapted from ISO 14971]

2.5
patient
any person who is subject to, or who utilizes, a health software product

NOTE In this Technical Specification, this is taken to include healthy persons, where applicable (e.g. a healthy person accessing a knowledge database to obtain health-related information).

2.6
product
entire entity proffered to a user, including instructions for use and training, where applicable

2.7
risk
combination of the likelihood of occurrence of harm and the severity of that harm

[adapted from ISO/IEC Guide 51:1999]

See Clause 4.

2.8
risk analysis
systematic use of available information to identify hazards and to estimate the risk

2.9
risk class
classification of a health software product according to the underlying risk it might present to the safety of patients

2.10
safety
freedom from unacceptable risk of harm

[ISO/IEC Guide 51:1999]

2.11
tolerable risk
risk which is accepted in a given context based on the current values of society

[IEC 61508-4:1998]

3 Abbreviated terms

ICT Information and Communication Technologies

4 Principles of hazard and risk analysis

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

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

There are a variety of approaches to hazard and risk analysis, all of which share a set of underlying concepts. Existing standards, guidance and publications tend to focus on particular sectors of activity (e.g. electronic safety systems, aeronautics) or subject areas (e.g. financial risks, risks to property, risks to the security of personal data). As such, they need interpretation in the context of health software products. This Technical Specification draws on a variety of sources to keep in line with accepted general principles. The Bibliography provides a list of useful sources of information on the subject. In considering the approach to take for health software products, account has been taken of how medical devices are classified and controlled in terms of safety. Annex A addresses this matter.

The following presents some of the basic concepts insofar as they are utilized in this Technical Specification. This clause is not intended to cover all aspects of hazard/risk analysis.

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

NOTE 1 ISO Guide 51 defines risk as the “combination of the probability of an event and its consequence”, whereas this Technical Specification defines it as the “combination of the likelihood of occurrence of harm and the severity of that harm” (2.7). The probability that a hazard will be realized might, in some domains, be represented quantitatively as a probability which may be based on historical or experimental failure analysis and incident statistics. That is very unlikely to be the case with health informatics products safety, where such statistics and evidence are not available, and therefore qualitative judgements are necessary. Whereas probability can of course be qualitatively expressed, the term “likelihood” better conveys that meaning and is therefore used in this Technical Specification.

NOTE 2 ISO Guide 73:2002 defines risk as the “combination of the probability of an event and its consequence”. This has the same drawback regarding the use of the term “probability” rather than “likelihood”. Moreover, this Technical Specification is focussed only on events that are likely to cause harm to patients and the severity of that harm, rather than other events. Thus, the term “event” is not used.

The consequence, i.e. harm to the patient(s), may take on different forms, varying from death to minor inconvenience, for example. Consequences may be categorized. Such categories need interpretation according to their sphere of application, in this case the application of ICT to health. This Technical Specification proposes five “consequence” categories, each with a description of its scope (see 5.2).

The likelihood that a hazard will be realized in reasonably foreseeable circumstances might, in some domains, be represented quantitatively as a probability which may be based on historical or experimental failure analysis and incident statistics. That is very unlikely to be the case with health software products safety, where such statistics and evidence are not available, and therefore qualitative judgements are necessary. This Technical Specification proposes five likelihood categories, each with a description of its scope (see 5.3).

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

Table 1

		Consequence				
		worst				least
Likelihood	highest	1	2			
		3				
						4
	lowest				5	6

Each cell of the matrix thereby represents a level of risk. Thus, in the risk matrix in Table 1 (above), the 25 cells represent 25 risk outcomes which reduce in severity on moving diagonally from top left to bottom right.

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

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

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

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

This Technical Specification proposes five risk classes (see 5.4).

5 Assignment of a risk class to a health software product

5.1 Introduction

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

5.2 Assignment to consequence categories

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

— catastrophic;

— major;

— considerable;

— significant;

— minor.

NOTE It will not be necessary to identify and categorize all possible consequences that could arise. The analysis to identify the realistic consequences and the likelihood of their occurring only needs to be undertaken to the extent required to assign with confidence the product to a risk class by means of the iterative process described in 5.6.

The consequence categories shall be interpreted as in Table 2. The descriptions have been created to suit the context of this Technical Specification, but are consistent with those in other sectors and in other complementary disciplines and approaches (see References [15], [16] and [17]).

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

Table 2

Consequence 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

In identifying the hazards that 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 that a health software product may present to a patient if it were to malfunction or be the cause of an unintended event, a hazard shall also not be dismissed simply because, even if it were to arise, no adverse consequences to a patient would occur, e.g. as a result of the vigilance of the user or other events external to the product. This aspect is addressed by the assignment of likelihood to the consequence occurring, as described in 5.3 and 6.5.

5.3 Assignment of likelihood to consequences

For each consequence identified, the likelihood of the consequence(s) occurring in reasonably foreseeable circumstances shall be assessed.

NOTE As pointed out in 5.2, it will not be necessary to identify all possible consequences that could arise. The analysis of possible consequences and the assignment to them of a likelihood of them occurring only needs to be undertaken to the extent required to assign with confidence the product to a risk class by means of the iterative process described in 5.6.

Each likelihood shall be assigned to one of the following categories:

— very high;

— high;

— medium;

— low;

— very low.

The likelihood categories shall be interpreted as in Table 3 (below). The descriptions have been created to suit the context of this Technical Specification, but are consistent with categories in other domains, e.g. corporate governance in healthcare (see Reference [18]).

Where there is doubt on the margins of two categories, the likelihood shall be assigned to the category of the higher likelihood (see Table 3).

Table 3

Likelihood category	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 but occur.
Low	Could occur, but in the great majority of occasions will not.
Very low	Negligible or nearly negligible possibility of occurring.

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 [see definition of **product** (2.6)]. In the context of this subclause, “likelihood” does not refer to 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. For example, if 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:

a) of the hazardous event being noticed by a user with appropriate qualifications before the consequence occurs;

b) of the consequence being avoided because the number of events over a period of time that would take place before the consequence resulted would enhance the possibility of the hazard being identified;

c) 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 circumstances that may reasonably be taken into account when assigning a likelihood shall be tempered by the severity of the consequence in question; the criteria being more stringent the more severe the consequence.

It shall not be permissible to assume best circumstances in all cases. For example, it is not permissible to assume that the operator is always highly competent and/or experienced, since it is reasonably foreseeable that circumstances will arise in which the product is used by an operator for the first time and that some operators, even with training, may be only marginally competent. Accepting these circumstances as a possibility is obviously important when a possible consequence is severe, such as death.

5.4 Risk classes

This Technical Specification is based on the concept of risk classes, each of which represents a combination of consequent categories and likelihood categories. Five risk classes are proposed: Classes A to E.

Each comprises a grouping of consequence and likelihood combinations which broadly represent the same level of risk to the safety of patients. Class A represents the highest potential risk and Class E the lowest.

The combinations that derive the risk classes are defined by Table 4.

NOTE Deciding which cells in the table are grouped together into a class is a matter of judgement based on consideration of the meanings assigned to each category of consequence and likelihood. The validity of Table 4 therefore requires experience of its application to different health informatics application sectors and of the manner in which the classes might be used in determining the controls which might be applied to products in the different classes to assure their safety. This experience will be important when this Technical Specification is reviewed for possible conversion to a full International Standard.

Table 4

		Consequence				
		Catastrophic	Major	Considerable	Significant	Minor
Likelihood	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

5.5 Assignment of risk class to a health software product

Consequence and likelihood combinations shall be assigned to a risk matrix as described in 5.4, utilizing the iterative process described in 5.6. The risk class of the health software product shall be the highest identified, where Class A is the highest and Class E is the lowest.

5.6 Process of iteration

The risk class into which a product falls depends on the combination of consequence category and likelihood category. Thus, a high consequence category combined with a low likelihood might result in a lower risk class than a lesser consequence category, but with a higher likelihood. Although any analysis will most likely focus at the outset on realistic worst consequences, it will also be necessary to consider lesser consequences to the extent of being confident, by a process of iteration, that the highest of the resulting risk classes is finally assigned to a product.

6 The analytical process

6.1 General

This clause lists some of the processes which should be considered in the analysis leading to the assignment of risk class.

6.2 Involvement of stakeholders

It will be essential that any analysis is founded on a clear and suitably in-depth understanding of the system, the environments in which it will be used and the users for which the system is intended. Agreement and decisions should be obtained from representatives of key stakeholders in the health software product. This might best be achieved by assembling a group representing at least:

— those engaged in system design, development and maintenance;

— users;

— those engaged in the business or process environment within which the system will be used.

It might also be advantageous if the group included representation or contribution from legal advisors and governance experts.

For products that are to be offered on a commercial basis, care should be taken to ensure the analysis is not unduly influenced by a sales view.

6.3 Understanding the system and user environment

The first step is for the team to reach a shared understanding of:

— the intent of the system;

— the environments in which it is intended to be used (environmental factors to be considered will be more than physical, e.g. the extent to which clinical expertise will be engaged);

— the system’s characteristics and modes of operation;

— the system/human interface;

— the dynamics of the processes with which the system will interface and which it will influence.

These matters shall be documented, including any scenarios considered and judged unreasonable.

6.4 Consequence analysis

In identifying what might happen if the system were to malfunction or cause an unintended event, and the consequences of this, the group should:

— ensure the process is business/profession/user driven, e.g. as opposed to being sales driven;

— ignore the system's underpinning controls and safety features;

— seek out the adverse events which would arise if the system malfunctioned, or was the cause of an unintended event, or was operated in an unintended manner, including:

  — human aspects (accidental and deliberate actions or inactions),

  — physical failures,

  — logical failures,

  — communication failures,

  — hardware failures, and

  - software failures;

- focus on scenarios considered to be “reasonable worst cases”;
- inform itself of actual incidents with the system and learn from them;
- inform itself of actual incidents with products of a like type and learn from the experience of others, including that reported in relevant literature;
- ensure all stakeholders are involved;
- encourage innovative thinking;
- seek out any underlying/eventual impact, not just immediate consequences;
- be imaginative but realistic;
- give full weight to the views of users and of those representing the healthcare environment in which the system is intended to be used.

6.5 Likelihood analysis

In assessing the likelihood of a consequence being realized in reasonably foreseeable circumstances, the group should:

- have before them the adverse events which could arise from a malfunction, etc., as used in assigning consequence categories;
- focus on the worst adverse events/consequences first;
- analyse the processes which might lead to harm to a patient arising from adverse events and the constraints working on those processes;
- consider past incidents that led to harm, including those reported in the “literature”;
- consider any likely changes and trends in the reasonably foreseeable future in the field in which the product is intended to be used;
- take into account, when considering human roles in likelihood:
  - motivation,
  - work pressures and opportunities,
  - competencies,
  - incentives and disincentives, and
  - work environment;
- seek out circumstances which might increase likelihood;
- avoid unreasonable confidence in professional or user competence in avoiding consequences;
- take account of the complexity of decisions or processes;

— take into account reasonable expectations of availability of resources, human and other, and particularly the impact of scarcity;

— take into account the interdependency of events in a chain;

— take into account the time lag between an adverse event arising from the system and any consequence possibly taking place;

— take into account the volume of activity being handled and the extent of remoteness of any consequences from operators, e.g. a “call and recall” system for breast screening may handle many thousands of patients, raising the statistical likelihood of a consequence being realized if that malfunction affected large numbers, all of whom would be remote from those operating the system and probably having little or no means of recognizing that an adverse event had occurred.

6.6 Iteration

As pointed out in 5.6, the risk class into which a product falls depends on the combination of consequence category and likelihood category. A high consequence category combined with a low likelihood might result in a lower risk class than a lesser consequence category, but a higher likelihood. Thus, although any analysis will most likely focus at the outset on worst consequences, it will also be necessary to consider lesser consequences and their likelihoods. However, not all consequences and their likelihood need be considered as long as, by a process of iteration, a point is reached whereby there can be confidence in the risk class assigned, i.e. that no other combinations of consequence and likelihood could result in a higher risk class.

6.7 Reviews

Changes in the design of a product or the field of intended application will take place from time to time, e.g. in the following situations:

— the introduction of new or changed functions;

— marketing into a new environment (e.g. taking a research system into a wide general market, opening a market in a new country, targeting a different clinical speciality, healthcare environment or type of organization);

— the introduction of new or changed interfaces with other systems.

Changes of this type may change the risk class to which a product should be assigned.

Reviews shall be undertaken as appropriate, both periodically and when any change takes place or is considered, which might affect the product’s risk class.

6.8 Documentation

The analytical process shall be fully documented, including:

— the malfunctions and adverse events considered and their consequences, including those rejected as unreasonable;

— the analysis of likelihoods to be assigned to consequences, including scenarios rejected as unreasonable;

— the iterative process and the logic which led to the assignment of the risk class with confidence.

This documentation should be seen as core system documentation, whose continued availability and currency should be assured.

6.9 Incident library

Judgements on reasonable consequences and their likelihood will be greatly assisted by reference to an incident library; therefore there shall be a means for collecting and storing such incidents.

7 Examples of assignment of risk classes to products

Annex B gives examples of the process for assigning a risk class to different types of health software product.

8 Relationship of risk classes to design and control of production of products

An important application of this Technical Specification will be the assignment of risk classes to different types of health software products, in order to group them for the purposes of presenting guidance, or a standard, for the design and production of such products. The nature of those controls and the rigour with which they need to be applied will depend on the risk class into which the product falls. Although it is not the purpose of this Technical Specification to specify what these controls should be for any risk class, an illustration of the nature of the relationship between risk classes and potential controls for risk management is given in Annex C.

Annex A
(informative)

Health software products and medical devices: rationale

A.1 General

In many countries, the safety of medical devices is assured through legislative provisions. The extent to which software is encompassed by such controls differs in some details but generally, by definition and by practice, software is covered only insofar as it is “necessary for the proper applications of a medical device” or is an accessory to a medical device.

In practice, at least at present, **health software products** (2.3) are not covered by such controls, examples being GP systems, call and recall, research data bases, e-prescribing software, ambulance dispatch systems, etc.

In considering a classification for health software products, it makes good sense to examine the approach taken with medical devices and, in that field, the relationship between classifications and controls for assuring safety, so that as far as practicable the approaches are on the same lines. This Annex considers these matters briefly. In the interests of brevity, no attempt is made to provide an in-depth analysis, and a number of complex issues and definitional matters have been simplified.

With medical devices, the approach is:

— first, broadly to classify devices with classes based on perceived potential risk to patients (typically four classes with sub-divisions);

— second, to apply controls on matters such as design, production, quality systems, labelling, etc., where the extent of the controls, and the rigour of their application, depends on the class: the higher the risk class the stronger the controls.

In this scenario, the issue of “risk” arises in two very different contexts: i.e. in the classification and in quality systems controls.

The classification system is founded on the perceived potential “risk” to patients. However, for medical devices, the assignment of class does not require a risk analysis *per se*. The assignment essentially depends on a device's applications, e.g. invasive, non-invasive, active, whether there is contact with the skin or not, whether energy is delivered to the body, etc. The classification is based on the premise that, with certain exceptions, invasive devices are of a higher potential risk than non-invasive devices. Health software products cannot be characterised by such terms as “invasive” or “active”, or whether they come into contact with the skin. Thus, the classification systems used for medical devices are not suitable for health software products.

In contrast, a usual control measure is the requirement for a manufacturer to have a satisfactory quality system. Part of this would be a requirement for risk management and to conduct a full and in-depth risk assessment of a device, and to mitigate risks to an acceptable level.

This Technical Specification is concerned with risk only in the context of a classification system for health software products and, as such, considers in broad terms the potential risk to patients of such products. This Technical Specification does not consider control measures for assuring the safety of health software products. However, it recognizes that if control measures are to be implemented, a prior necessity is to classify health software products to allow controls to be proportionate to the risk to patient safety. Controls might of course include the requirement for a quality system and, within that, a requirement to apply a full risk assessment process to a product and to mitigate risks to an acceptable level. Risk analysis in this context is not, however, the subject of this Technical Specification.

It makes sense to examine whether the classification systems used in the context of medical devices could be applied to health software products. The conclusion is that they cannot: hence the need for this Technical Specification for the reasons given in this Annex.

A.2 FDA guidance relating to software

In the U.S.A., the FDA (Food and Drug Administration) has issued guidance on software encompassed by medical device controls. It contains material of significance to this Technical Specification.

Reference [20] 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 pre-market 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 recognizes three levels listed below.

a) Major The level of concern is 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 to the patient or operator through incorrect or delayed information or through the action of a care provider.

b) Moderate The level of concern is 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.

c) Minor The level of concern is 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; or

— 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".

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 Technical Specification proposes the same requirement (see 5.2 and 5.3).

FDA CDRH (Centre for Devices and Radiological Health) guidance on off-the-shelf software use in medical devices [21] contains the following 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]. Based on the definition of Risk Analysis in ISO 14971 and EN 1441, 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 then the software failure rates."

Reference [21] also proposes a classification based on "level of concern", with definitions which are substantially the same.

It should be noted that the guidance on software in medical devices clearly states that the guidance on "level of concern" applies only to pre-market submissions and is "not related to device classification (Class I, II, or III) or to hazard or risk analyses *per se*". Nevertheless, the question arises as to whether this classification would serve the purpose of health software products and this Technical Specification.

Like the FDA guidance [20], this Technical Specification recognizes that, with software, the issue is systematic faults and that risk cannot be based on software failure rates. In essence, if a fault is there, it will manifest itself at some point, i.e. the probability of its occurrence is essentially 100 %. Thus, for software, a risk analysis boils down to a hazard analysis, i.e. the identification of the nature and severity of potential harm when a systematic fault manifests itself. This Technical Specification categorizes the nature and severity of such potential harm in "five consequence categories" (rather than the three used by the FDA), in order to provide somewhat greater delineation, and does not cover operators. It is also more comprehensive in its definition of consequences, e.g. it recognizes a difference between harm to a single patient and harm to multiple patients, and specifically includes psychological trauma. The latter could, for example, be substantial with malfunction of security provisions in a research data base of person identifiable HIV cases. Nevertheless, the terms used in this Technical Specification are similar to those used in the FDA guidance [20].

The FDA guidance does not, however, address the question as to whether, when an adverse event occurs with the potential to cause harm, that harm will in practice be realized in reasonably foreseeable circumstances. For example, in the case of a software system designed to issue reminder letters to patients about appointments that have been made for them with an outpatient department, if the software malfunctions and fails to issue a letter, it can be argued that harm to a patient could arise due to missing the appointment. Nevertheless, the probability of harm arising in practice is remote, in that the patient is aware of the appointment, will take action when he/she realizes it has been missed, and the missed appointment will be noticed by the outpatient clinic when it occurs such that action can be taken to fix a further appointment. On the other hand, if a call and recall system malfunctions and fails to issue a recall letter to a patient with an adverse test result, not only could the patient be harmed, but the probability of the harm actually being realized could be high, i.e. the patient will not be aware that a recall was necessary and the system will not recognize that the patient has not been contacted. It is reasonable to distinguish such examples in terms of assigned risk class.

Thus, this Technical Specification proposes assigning a likelihood to harm actually being realized in foreseeable circumstances once an adverse event with potential for harm has arisen.

It is important to recognize that whilst the 5×5 matrix defining the five risk classes (see 5.4 and Table 4) has the appearance of a classic risk chart matrix which might, for example, arise from a risk analysis of a medical device in a quality system (e.g. as in ISO 14971), the "likelihood" axis has a fundamental difference. The likelihood axis in this Technical Specification is not the qualitative probability that an adverse event will occur in a health software product. It is the likelihood that the consequences of that adverse event will be realized in practice once that event has taken place. Assessment of this aspect of this Technical Specification will be particularly necessary when this Technical Specification is reviewed for possible conversion into a full International Standard.

Annex B
(informative)

Examples of assignment of Risk Classes

B.1 General

This annex is only an indication of the process of assigning a risk class to different types of health software products. It contains examples and, as such, shall not be taken as the definitive assignment of risk class for such products.

B.2 Hospital e-prescribing system with decision support

When assigning a risk class to hospital e-prescribing systems with decision support, the first step is to consider what the consequences could be if such a system malfunctioned or failed to operate as intended, or what the cause of an unintended event could be.

An unintended event might be the generation of a prescription for a drug with one or more of the following:

— wrong person;

— wrong drug;

— wrong dose;

— wrong repetition;

— wrong route;

— wrong timing;

— unforeseen drug-drug interaction;

— unforeseen allergic reaction to drug.

The above unintended events might be compounded by an error in the placing of a decimal point in the prescribed quantity or the generation of a prescription for a drug of type or quantity which is inappropriate for the particular type of patient, e.g. for a child. Whereas many of these events could result from a malfunction of a system, they are more likely to occur because the user unintentionally enters the wrong information through ignorance or a slip in concentration. These adverse events cannot, however, be dismissed purely as user error, since the design intentions in these systems will be to provide appropriate alerts in these circumstances. The fact that such potentially harmful prescriptions may be generated may thus be due as much to failure or inadequacy in the decision support system as to simple user error.

It is not permissible for a vendor to dismiss the possibility of such events because of the belief that his product is so well designed that such events could not occur. In a recent study [19], 18 potentially hazardous scenarios were used to test four well-established GP systems used in three-quarters of GP practices in the U.K. The systems were designed to give drug interaction alerts. However, none produced alerts for all 18 scenarios: the best produced seven alerts and the worst four. In terms of prescriptions of drugs with similar names, none of the systems gave warnings for all the ten drug pairs considered. The manufacturers of each of these systems may have believed that all hazardous circumstances were covered within their designs, but they were not.

The next step is to consider what might be the consequences of such events. In this example, it is easy to envisage circumstances where, should an “erroneous” prescription be dispensed and administered, death or severe injury (from which recovery could not be expected in the short term) could occur. These consequences fall into the consequence category “major”.

The next step is to assess the likelihood of these consequences of death or serious injury being realized in “reasonably foreseeable circumstances”. Such “reasonably foreseeable circumstances” will involve consideration of a chain of events involving the passing of a potentially harmful prescription from the doctor in charge to a dispenser to the drug administrator, and its actual administration to a patient, with the consequence then actually being realized. Assessing the likelihood of death or serious injury actually occurring will therefore involve a reasonable assessment of whether the deficiency in the prescription will be noticed and corrected somewhere along the chain and whether, even if the prescribed medication were administered, death and/or serious injury would be avoided. It is not permissible to assume best or perfect conditions anywhere in the chain, e.g. to assume that all those in the chain are highly competent, alert clinicians. On the other hand, the likelihood that there are totally incompetent staff all through a chain might be an unreasonable assumption. However, it is a requirement that what may be taken into account as reasonable when assigning a likelihood shall be tempered by the severity of the consequence in question, the criteria being more stringent the more severe the consequence. In this example, the possible consequence is extremely severe.

In practice, it is known from experience that once a potentially harmful prescription has been generated, it can be and has been administered and death and serious injury have resulted. The assigned likelihood category would thus be either “very high” or “high”. When placed in the risk matrix, the combination of “major” consequence category combined with the likelihood category “very high” results in e-prescribing systems with decision support being assigned to Class A. However, the combination of “major” consequence category and likelihood category “high” results in an assignment of Class B. The assignment of class is resolved by the requirement that “where there is doubt on the margins of two categories, the likelihood shall be assigned to the category of the higher likelihood”. This settles the class as Class A.

No further analysis (iteration) is required since it is necessary to conduct an analysis “only to the extent necessary to assign, with confidence, the product to a risk class” and there is no “higher” risk class than Class A.

The assignment of Class A to e-prescribing systems with decision support is not surprising, since it can readily be recognized that serious harm can result to patients if they are poorly designed. Any guidance, standards or regulations on controls that should be exerted on the design and production of health software products would also be expected to be most stringent for health software products of this type (Class A) because of their potential for serious harm if not subject to such stringent attention.

B.3 Bar code case note tracking system

This example is based on a system that generates a bar code label which will uniquely identify a patient's paper case notes so that, when case notes are moved from one location to another within a hospital, they can be checked in and out with a bar code reader, and their location can thereby be identified.

The first step is to consider what might happen if such a system should malfunction or be the cause of an unintended event.

One malfunction might be the failure of the system to track a particular set of notes, with the result that they cannot be traced and are thereby not available to the clinician when required. The consequence of this circumstance will depend on the clinical situation applying when the notes cannot be found.

Even though even a moderately competent clinician might be expected to be cautious and delay action until sufficient information had been ascertained by some means, it might nevertheless be argued that a consequence could occur in the major or considerable categories, but that the likelihood of such consequences actually being realized would be “very low”. This indicates Class C.

Some might regard this as too severe a judgement, and that in practice the possible consequences would more reasonably lie in the significant or minor categories, with a likelihood of medium or low. This would indicate Class D or E.

Further considerations would be needed, including perhaps a literature search, in order to finalize the Class (either C, D or E).

This would appear reasonable. Any guidance, standards or regulations on controls that should be exerted on the design and production of such health software products (Classes C, D, E) would be unlikely to impose conditions as severe as for an e-prescribing system with decision support (Class A).

B.4 Research system for sexually transmitted diseases

This example is a system designed “in house” for holding and analysing research data in the context of sexually transmitted diseases. The system holds patient identifiable data.

The first step is to consider what might happen if the system were to malfunction or fail to operate as intended.

Such a system will not be used for direct patient care and therefore events leading to consequences such as death, serious or minor injury are not applicable. However, failures to adequately protect the confidentiality of patient data can be envisaged, e.g. through lack of, or deficiencies in, access control or poor password requirements. Thus, the identity of a patient with a sexually transmitted disease such as HIV might be revealed to an unauthorized person or persons. A consequence could then be “significant” psychological trauma to the patient, i.e. in the “significant” consequence category.

The next step is to consider the likelihood of the consequences actually being realized. Physiological trauma for a patient will not arise unless the patient concerned becomes aware of the breach in confidentiality. This will depend on the circumstance of the unauthorized access. If the unauthorized access was by a clinician who, without intent, found him/herself viewing such sensitive information, that clinician, because of his/her general duty to preserve confidentiality, would be very unlikely to pass on such information to any other person. However, accidental or unauthorized access by a person not bound by such an obligation could result in idle or malicious chatter, especially if the patient in question was known in the local community. Nevertheless, a long chain of events could reasonably be expected before a patient would learn of the incident, and the likelihood might be judged as medium to low. Either results in either Class D.

An additional consideration would apply if the system had an audit trail which exposed the fact that unauthorized access had occurred. The system “owner” might in these circumstances be obliged to inform the patient that such a breach had taken place. This would mean that the likelihood of the consequence being realized would be “very high”. However, it could reasonably be argued that the psychological trauma experienced by the patient may be lessened by virtue of being informed and counselled by a responsible clinician. Psychological trauma might thus be judged as “minor” rather than “significant”. The result would be Class C.

These arguments point to either Class C or D. If there is significant doubt as to which should apply, the requirement is to assign the higher class, i.e. Class C.

NOTE For a research system holding far less sensitive data, the most that might be expected would be minor psychological upset (if any), with a likelihood of low or very low, i.e. Class E.

It is not surprising that a system holding person-identified, very sensitive health data, such as sexually transmitted diseases, should be in a relatively “high” class. Any guidance, standards or regulation on controls that should be exerted on the design and production of health software products in this class (C) can be expected to be fairly stringent, in this example focusing on data protection, security and access control.

B.5 Ambulance service despatch system

The area of emergency services inevitably carries with it an assumption of “life and death”, but the reality can in fact differ from this. Whilst the development of “leading edge” solutions for ambulance service despatch [such as the example of the London Ambulance Service in the mid-1990s[1)]] do indeed deliver such impacts, earlier generation systems (which do not, for example, assign crews based on their particular skills and/or response units based upon specialist equipment) are much more “supportive” than “directive”. Such a system is considered here.

When considering the realistic worst case impact, the probable circumstances of a call to an ambulance service that leads either to a crew not being despatched or to a crew being despatched to the wrong location need to be identified.

For a death to occur, the assumption would be that the patient condition is critical and that there were no other persons available to make the call and to follow up. In circumstances such as an individual being alone and suffering a major heart attack, a call is not even likely to be made. If a death were to result, this would not be related to the despatch system. In the case of a major car crash, wounding in a fight, building collapse or other “major incident”, there would be representatives of one or more of the emergency services in attendance. These individuals can be expected to be able to identify accurately the location and follow up responses. Again, whilst there might be deaths before the emergency services get to the scene or immediately after their arrival, these are again not attributable to the ambulance service despatch system.

Therefore, for this scenario, the impact is likely to relate to an individual with a material injury, or a group of injured containing such within their number, where the response vehicle is delayed or is not despatched, causing the condition to worsen and/or the recovery, which could normally be expected with confidence, to take longer. This could conceivably leave the patient with severe incapacity and/or severe psychological trauma. This matches closely to the definition for “considerable” consequence.

Consideration of the likelihood of the worst case impact then occurring is a complex one. A failure to despatch a unit, to delay that unit or to despatch it to the wrong location (thereby delaying their arrival at the right location), could be caused by:

a) a delay in the emergency call being made (not the responsibility of an ambulance service);

b) a delay in the dispatcher replying to the call (many possible component failures of lack of capacity, e.g. in incoming phone lines);

c) error or imprecision on the part of the dispatcher when entering the address and/or postcode details (because of poor signal or typographical error);

d) the assignment of a unit for response that is unavailable (already on a call, on rest break or other reason);

e) a dispatch message failing to reach the response unit (not related to the core despatch system).

For item b), the likelihood is considered to be “very low”. There is typically high bandwidth made available by telephone companies for emergency services and, whilst such bandwidth might be argued to be a control or countermeasure, it is one that is so well understood that it is part of normal operations.

For item d), assuming the system has no intelligence in this area or that it is defective, the likelihood can be considered to be “low”, as it can be assumed that the crew will quickly state that they are unavailable to “deal”.

The failure that is of concern is item c). The system may not be equipped with the capability to look up post code and/or to cross check addresses and postcodes, or the functionality may fail or be corrupt. Post codes are, of course, very similar to each other, without a transparent logic and too numerous for a dispatcher to memorize in a location context. The likelihood here is at least “high”, but could conceivably be considered “very high”.

---

1) See LASCAD Case Study available at: http://www.cems.uwe.ac.uk/teaching/notes/UQI101S2/lascad.htm.

The combination of “considerable” consequence with “very low”, “low” and “high” likelihoods derives risk classes of “D”, “C” and “B” respectively. Even the “very high” likelihood still only derives a risk class of “B”, making this the realistic worst case.

In practice, therefore, the failure risks summarized in item c) above should be separated and considered individually, even though none of them could increase the risk measure above risk class “B”. In the light of the “high” and “very high” likelihoods derived, the focus should be on the consequence assessment to ensure that there are no “major” or “catastrophic” scenarios. If there are, then a risk class of “A” would be derived.

Annex C
(informative)

Illustration of the nature of the relationship between risk classes and potential controls for risk management

C.1 Use of risk classes

The purpose of assigning products to risk classes in the manner proposed in this Technical Specification is primarily to make a broad distinction between:

a) those products which could present a severe risk to patients if they malfunctioned,

b) those products that would not present a severe risk to patients if they malfunctioned, and

c) those products that lie between these extremes.

Those in a high risk class (such as Class A) evidently require stringent attention to ensure that the risks which they could present to patients do not materialize.

Minimizing the possibility that risks will materialize may be achieved in several non-exclusive ways, e.g. by:

— controls on the design, production, maintenance and upgrading of a product (including instructions for use), to ensure as far as is practicable that adverse events which might lead to harmful consequences do not arise in practice;

— training and retraining of users to ensure that they are aware of possible risks and are alert to possible adverse events, thereby preventing the consequences to which events might have led;

— instigating administrative controls and checks within the environment in which the system operates, or with which it interfaces, so that adverse events can be spotted and consequences avoided or reduced.

Thus, those responsible for overall risk analysis and risk reduction in a healthcare establishment may wish to identify those health software products on which they should concentrate when making purchasing decisions, implementation and use, and in reviews of operating procedures. They will not wish to apply the same attention to, or apply controls with the same rigour to, products in Classes D or E as they might for those in Classes A or B.

Those responsible for drafting guidelines, standards or regulations on the controls deemed necessary on the design and production of health software products will wish to distinguish between those types of product which, if not adequately controlled, would present most risks from those that present lesser risks. The most stringent controls to be applied with the most rigour would be required of Class A, and the least (perhaps none) for Class E.

Regulators and standard makers may find five classes too fine a gradation, and might combine classes for the purposes of applying distinguishable “packages” of control requirements. Thus, for the purposes of specifying necessary controls, regulators may choose not to distinguish between Classes A and B, or between Classes C and D.

It is not the purpose of this Technical Specification to define the controls necessary to avoid or mitigate the consequences to patients according to a product's risk class. However, it is evident that, for products in the higher risk classes, a very much more detailed and rigorous analysis would be necessary to identify necessary risk reduction measures than is necessary solely to “screen” them and to assign them to one of the broad risk classes in this Technical Specification.

C.2 Fundamentals

The risk classification derived from the assessment process (formed as it is from an assessment of the possible impact on, or harm to, a patient, and of the likelihood of that occurring) will provide a justification for any controls recommended for ensuring product safety. This justification will apply to both the volume and rigour of controls, such that a hierarchical and layered controls library would be required.

The risk classification process does not consider issues such as technical architecture, or factors such as dependency. Therefore, the risk classification does not provide any justification of applicability. Whilst this issue should be considered further in any guidance or standards on controls, it infers that users of the risk classification process will need to make such assessments manually and on an experiential basis.

The varying extent of controls consequent to the risk classification process may include no recommendations being made in certain control areas where the risk class is low. In contrast, for products assessed as a high risk class, requirements should be expected to be rigorous and should require such tasks as independent evaluation, formal design, extensive testing, etc.

The risk classification process is not intended as a substitute for more broadly-based and detailed risk assessment. Indeed, the latter is fundamental in ensuring that the infrastructure and environment within which the health software product is resident is commensurate with the risks. For example, in the context of information security, this related process will identify requirements for such controls as virus protection, message security, network security, data confidentiality over networks, etc. Indeed, the resulting combined requirements are likely to involve interactions/interfaces/interoperability of the health software product to enable this, in its own interest.

C.3 Controls group examples

The types of controls that are likely to need to be considered when undertaking the management or treatment of the identified “risk classification” are the following:

— additional risk classification activity;

— related security risk assessment activity;

— programme management;

— programme risk management;

— design facilities;

— management of system design;

— system designer competence and experience;

— information display and presentation rules;

— design integrity;

— design assurance/validation;

— system development facilities;

— management of system development;

— system developer competence and experience;

— integrity controls;

— penetration testing/technical assurance;

— knowledge base development facilities;

— management of knowledge base design;

— management of knowledge base development;

— knowledge base assurance/validation;

— security policy development;

— resilience and redundancy requirements;

— identification and authentication;

— user access control;

— object reuse;

— storage requirements/capacity planning;

— back-up requirements;

— accounting and audit;

— equipment failure protection;

— incident management;

— business continuity management;

— testing of systems development;

— formal evaluation of developed systems;

— development of operating procedures;

— development of maintenance procedures;

— development of user procedures;

— training of staff;

— management supervision.

This list is not intended to be definitive, and would need a material level of further analysis and design before it could be adopted in any further guidance or standards. The extent to which the types of controls listed above might be required, and the rigour with which they needed to be done, would depend on the risk class.

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 Organization 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] 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

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

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

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

[11] ISO 14971, *Medical devices — Application of risk management to medical devices*

[12] IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*

[13] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[14] ISO/IEC Guide 73:2002, *Risk management — Vocabulary — Guidelines for use in standards*

[15] UK Government Information Security, Risk Analysis and Management Method (CRAMM) User Manual, CCTA, (now part of the Office of Government on Commerce) Publisher Central Computer Telecommunications Agency

[16] ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

[17] AS/NZS 4360:1999, *Risk Management*

[18] Corporate governance in health care Qualitative Measures of Likelihood of Risk, Department of Health, England

[19] FERNANDO, B., SAVELYICH, B., AVERY, A., BAINBRIDGE, M., HORSFIELD, P and TEASDALE, S., Prescribing safety features of general practice computer systems: evaluation using simulated test cases, *BMJ*, May 2004, **328**, pp. 1171-1172

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

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

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

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

ICS 35.240.80

Price based on 24 pages