NHS
Connecting for Health

Health Informatics — Application of clinical risk management to the manufacture of health software (formerly ISO/TS 29321:2008(E)) – DSCN14/2009			
Programme	NPFIT	**Document Record ID Key**	
Sub-Prog / Project	Clinical Safety	NPFIT-FNT-TO-TOCLNSA-0830.01	
Prog. Director	Professor Michael Thick	Status	Issued
Owner	Dr Maureen Baker Debbie Chinn	Version	1.0
Author	Ian Harrison	Version Date	April 09

Health Informatics — Application of clinical risk management to the manufacture of health software Formerly ISO/TS 29321:2008(E) DSCN14/2009

Amendment History:

Version	Date	Amendment History
0.1	April 09	First draft for comment
1.0	June 09	Approved by named approvers

Forecast Changes:

Anticipated Change	When
IEC 80001 to Supersede in Summer 2010	Summer 2010

Approvals:

This document must be approved by the following:

Name	Signature	Title / Responsibility	Date	Version
Professor Michael Thick	Via Email	Chief Clinical Officer	June 09	1.0
Dr Maureen Baker	Via Email	Clinical Director for Patient Safety	June 09	1.0
Debbie Chinn	Via Email	Director of National Integration Centre	June 09	1.0

Distribution:

This document will be distributed on request to internal and external colleague for the purpose of Clinical Safety Management.

Document Status:

This is a controlled document.

Whilst this document may be printed, the electronic version maintained in FileCM is the controlled copy. Any printed copies of the document are not controlled.

Related Documents:

These documents will provide additional information.

Ref no	Doc Reference Number	Title	Version
1	NPFIT-FNT-TO-TOCLNSA-0831.01	Health informatics - Guidance on the management of clinical risk relating to the deployment and use of health software (formerly ISO/TR 29322:2008(E))	1.0
2	NPFIT-SHR-QMS-PRP-0015	Glossary of Terms Consolidated	13.0

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

- an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;
- an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

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

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

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

Note: NHS CFH Clinical Safety Group, in agreement with the NHS Information Standards Board, have issued this paper as a cover document for TS29321 the ISO/CEN technical specification which despite considerable international support, failed to gain the necessary votes for approval in December 2008. The NHS believes that it is vital that health systems are properly covered by safety standards commensurate with their level of criticality and patient safety risk. To this end, the document formerly known as ISO/TS 29321:2008(E) will be used as an NHS standard for health systems not formerly covered by Medical Devices approval. This document will act as an interim safety standard until 2010, when a new ISO/CEN health system safety initiative is expected to supersede TS29321.Any references to TS29321 in this document should be considered references to the document itself. A similar piece of work is being done under a DSCN for TR29322 - Health informatics -- Guidance on the management of clinical risk relating to the deployment and use of health software systems - this will be available shortly.

Introduction

The threat to patient safety

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

It is increasingly claimed that information systems such as decision support, protocols, guidelines and pathways could markedly reduce such adverse effects. If for no other reasons – and there are others – this will lead, and is leading, to increasing utilization of decision support and disease management systems which inevitably will increase in sophistication and complexity. It can also be anticipated that, due to pressures on time and medico-legal aspects, clinicians will increasingly rely on such systems with less questioning of their "output". Indeed, as such systems become integrated with medical care any failure to use standard support facilities may be criticised on legal grounds.

Increased decision support can be anticipated not only in clinical treatment but also in areas just as important to patient safety, such as referral decision-making, where failure to make a "correct" referral or to make one "in time" can have serious consequences.

Economic pressures are also leading to more decision support systems. The area of generic and/or economic prescribing is the most obvious, but economy in number and costs of clinical investigative tests is another.

Systems such as those for decision support have considerable potential for reducing clinical errors and improving clinical practice, e.g. in the reduction in errors resulting from the deployment of electronic prescribing.

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

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

Harm can of course result from unquestioning and/or non-professional use although designers and suppliers can mitigate such circumstances through, for example, instructions for use, training and on-screen presentation techniques, guidance or instruction. The potential for harm may equally lie in the system design such as:

- flaws in the requirement for the use of the system;
- poor evidence base for design;
- failure in design logic to properly represent design intentions;
- failure in logic to represent good practice or evidence in the design phase;
- poor or confusing presentation of information or poor search facilities;

- failure to update in line with current knowledge.

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

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

Controlling the risks

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

A necessary precursor for determining and implementing appropriate design and production controls to minimize risks to patients from poor design, product malfunction or inadequate performance is a set of safety requirements. These should be derived from an initial set of hazards and require a clear understanding of the risks which a product might present to patients if malfunction or an unintended event were to occur, and the likelihood of such a malfunction or event causing harm to the patient. Additionally, if guidance is to be given to designers and producers of health software products as to design and production control (and corresponding standards produced) then it will need to be recognised that the controls necessary for products presenting low risks may not be the same, or applied with the same rigour, as for those presenting high risks. The controls which are selected need to match both the level and types of risk which a product might present to a patient. For these purposes many standards, legislation and specifications dealing with control of risks in design and production, group products into a limited number of classes or types according to the risk they might present. Controls are then tailored to the class or type. For medical devices such groupings are well established. For health software in 2006 CEN published EN TS 15260 [10] which, subject to validation of its risk classes in its Table 4, could provide a process for grouping health software based on risk characteristics.

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

Conclusion 8 reads:

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

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

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

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

ISO 14971 [13] is widely used throughout the world for compliance with medical device safety regulations.

Such regulations for medical devices in most countries encompass software that is necessary for the proper application of a medical device or software that is an accessory to a medical device. In some jurisdictions, medical device regulations also cover some other software. Thus medical device manufacturers have considerable experience in the application of ISO 14971. Many manufacturers, particularly of electrical medical devices, are experienced in the incorporation of software in medical devices, in producing software supporting such medical devices and/or producing software that is a medical device in its own right. A number of these manufacturers may also produce other health software of a type not encompassed by medical device regulations. It would be advantageous to such manufacturers and any regulators if the standard for the application of risk management to health software bore as close a relationship as practicable to ISO 14971.

This may in particular be an advantage in circumstances where software which is part of a medical device complying with ISO 14971, interacts with software not controlled as a medical device but compliant with this Technical Specification. Each may contribute a hazard to the other and thus access to the risk analysis for both may be necessary.

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

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

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

1 Scope

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

- necessary for the proper application of a medical device;
- an accessory to a medical device;
- a medical device in its own right.

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

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

NOTE 1: The scope is intended to cover health software products that are not controlled by medical device regulations.

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

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

- requirements capture and concept development;
- detailed design;
- production;
- software release/marketing;
- deployment;
- use;
- decommissioning.

A manufacturer is responsible for requirements capture and concept development, detailed design, production and software release/marketing and can be responsible for deployments particularly the first “go live” of complex systems.

Where a customer contracts out responsibility for IT services to the manufacturer, the latter may also be responsible for use of the application and its decommissioning. This Technical Specification applies to all the life-cycle phases for which the manufacturer is responsible where this will depend on the contractual scope with the customer.

NOTE 3: Failures and deficiencies in software products used in the health environment can, of course, have adverse impacts other than causing harm to patients. They might, for example, create administrative inconvenience with a range of impacts on the organization including financial loss. Harm to a patient may also have a consequent impact on the organization such as loss of reputation and/or financial loss resulting from litigation. Whereas these adverse organizational impacts will be significant to an organization, they are not the subject of this Technical Specification unless they can result in harm to a patient. It is the potential harm to the patient that is the subject of this Technical Specification.

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

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

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

2 Terms and definitions

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

2.1 Clinical hazard

Potential source of harm to a patient.

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

2.2 Clinical risk

Combination of the likelihood of occurrence of harm to a patient and the severity of that harm.

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

2.3 Clinical risk analysis

Systematic use of available information to identify and estimate a risk.

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

2.4 Clinical risk assessment

Overall process comprising a clinical risk analysis and a clinical risk evaluation.

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

2.5 Clinical risk control

Process in which decisions are made and measures implemented by which clinical risks are reduced to, or maintained within, specified levels.

2.6 Clinical risk estimation

Process used to assign values to the likelihood of occurrence of harm to a patient and the severity of that harm.

2.7 Clinical risk evaluation

Process of comparing the estimated clinical risk against given risk criteria to determine the acceptability of the clinical risk.

2.8 Clinical risk management

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

2.9 Clinical risk management file

Repository of all records and other documents that are produced by the clinical risk management process.

2.10 Clinical safety

Freedom from unacceptable clinical risk to patients.

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

2.11 Clinical safety case

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

2.12 Clinical safety case report

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

2.13 Clinical safety management system

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

2.14 OTS

Off-the-shelf software that is not health software.

2.15 Harm

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

NOTE: Adapted from ISO/IEC Guide 51:1999.

2.16 Hazardous situation

Circumstance in which a patient is exposed to one or more hazard(s).

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

2.17 Health software product

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

- necessary for the proper application of a medical device;
- an accessory to a medical device;
- a medical device in its own right.

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

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

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

2.18 Intended use

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

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

2.19 Life cycle

All phases in the life of a health software product, from the initial conception to final decommissioning and disposal.

2.20 Manufacturer

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

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

2.21 Medical device

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

- diagnosis, prevention, monitoring, treatment or alleviation of disease;
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury;
- investigation, replacement, modification, or support of the anatomy of a physiological process;
- supporting or sustaining life;
- control of conception;
- disinfection of medical devices;
- providing information for medical purposes by means of in vitro examination of specimens derived from the human body;

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

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

2.22 Objective evidence

Data supporting the existence or verity of something.

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

[ISO 9000:2005, definition 3.8.1]

2.23 Patient

Any person who is subject to a health software product.

NOTE: In this document that shall be taken to include healthy persons where applicable (e.g. a healthy person accessing a knowledge data base to obtain health-related information).

2.24 Pre-release stage report

Stage report produced and signed off by top management, before a health software product is released for distribution or deployment.

2.25 Post-production

Part of the life cycle of the product after the design has been completed and the health software product has been manufactured, prior to its release for use.

2.26 Post-deployment

Part of the life cycle of the health software product after it has been manufactured, released and deployed ready for use.

2.27 Procedure

Specified way to carry out an activity or a process.

[ISO 9000:2000, definition 3.4.5]

2.28 Process

Set of interrelated or interacting activities which transforms inputs into outputs.

[ISO 9000:2000, definition 3.4.1]

2.29 Product

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

2.30 Product liability

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

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

2.31 Record

Document stating results achieved or providing evidence of activities performed

[ISO 9000:2000, definition 3.7.6]

2.32 Residual clinical risk

Clinical risk remaining after risk control measures have been taken

NOTE: ISO/IEC Guide 51:1999 [30], definition 3.9 uses the term “protective measures” rather than “risk control measures”. However, in the context of this

Technical Specification, “protective measures” are only one option for controlling risk as described in 7.2.

2.33 Severity

Measure of the significance of the possible consequences of a hazard.

2.34 Stage report

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

2.35 Top management

Person or group of people who directs and controls a manufacturer at the highest level.

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

2.36 Verification

Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled [ISO 9000:2000, definition 3.8.4]

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

NOTE 2: Confirmation can comprise activities such as:

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

3 Abbreviated terms

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

EU	European Union
DBMS	Database Management System (Software)
GHTF	Global Harmonization Task Force
GP	General Practitioner
OTS	Off-The-Shelf
SOUP	Software of Unknown Provenance

4 General requirements for effective clinical risk management

4.1 Clinical risk management process

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

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

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

4.2 Management responsibilities

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

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

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

Top management shall:

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

and effectively applied; at each stage, top management shall sign off the appropriate stage report (see Clause 9);

- review the suitability of the clinical risk management process at planned, regular intervals to ensure continuing effectiveness of the clinical risk management process and document any decisions and actions taken.

This review should be linked to the manufacturer’s clinical safety management system which in turn may be part of its quality management system or its enterprise risk management system.

NOTE 2: The documents can be incorporated within the documents produced by the manufacturer’s quality management system and these documents can be referenced in the clinical risk management file.

4.3 Competencies of personnel

Persons performing risk management tasks shall have the knowledge, experience and competencies appropriate to the tasks assigned to them. This shall include, where appropriate, knowledge and experience of the particular health software product (or similar health software products) and all its applications, the technologies involved or risk management techniques. This should include an appropriate registered clinician.

Appropriate competency and experience records shall be maintained.

NOTE: Clinical risk management tasks can, and should, be performed by representatives of several functions, each contributing their specialist knowledge. Of particular importance will be clinical input from clinicians who are familiar with the practical realities of the environments within which the product will be used an the clinical processes to which the product is directed.

4.4 Clinical risk management planning

Clinical risk management activities shall be planned. Therefore, for the particular health software product being considered, the manufacturer shall establish and document a clinical risk management plan in accordance with the clinical risk management process. The clinical risk management plan shall be the part of the clinical risk management file.

This plan shall include at least the following:

- the scope of the planned clinical risk management activities, identifying and describing the health software product, the clinical context in which it will be used and the life-cycle phases for which each element of the plan is applicable and the life-cycle phases which the plans covers;
- assignment of responsibilities and authorities;
- requirements for review of clinical risk management activities;
- identification of relevant risk management procedures and processes to be used;
- criteria to be used in analysis of the risks;

- criteria for assessing clinical risk acceptability, based on the manufacturer's policy for determining acceptable clinical risk, including criteria for accepting clinical risks when the likelihood of occurrence of patient harm cannot be estimated;
- verification activities;
- activities related to collection and review of relevant production, post-production and post-deployment information.

NOTE 1: Refer to Annex E for guidance on developing a clinical risk management plan.

NOTE 2: The clinical risk management plan will be the first component of the clinical risk management file although not all parts of the plan need to be created at the same time. The plan or parts of it can be developed over time as the relevant risk management process requirements become better understood.

NOTE 3: The criteria for clinical risk acceptability are essential for the ultimate effectiveness of the clinical risk management process (See Annexes F and H).

NOTE 4: Clinical risk management planning needs to be based on a clear understanding of the context in which the health software is intended to be used.

If the plan changes during the life cycle of the health software product, a record of the changes shall be maintained in the clinical risk management file.

4.5 Clinical risk management file

For the particular health software product being considered, the manufacturer shall establish and maintain a clinical risk management file that shall be the repository of the documentation produced and shall provide suitable traceability. In addition to the requirements of other clauses of this Technical Specification, the clinical risk management file shall provide traceability for each identified hazard to:

- the requirements and objectives of the software development;
- the clinical risk analysis;
- the clinical risk evaluation;
- the implementation and verification of the clinical risk control measures;
- the assessment of the acceptability of any residual clinical risk(s).

NOTE 1: The records and other documents that make up the clinical risk management file can form part of other documents and files required, for example, by a manufacturer's clinical safety management system and/or quality management system. The clinical risk management file need not physically contain all the records and other documents; however, effective compliance will require it to contain at least references or pointers to all required documentation and version control references. The manufacturer should be able to assemble the information referenced in the risk management file in a timely fashion.

NOTE 2: The clinical risk management file can be in any form or type of medium.

NOTE 3: For the relationship between clinical risk management file, clinical safety case, clinical safety case report and clinical risk management close-out report and product life-cycle, see Annex G.

4.6 Clinical safety case

The manufacturer shall develop and maintain a clinical safety case for the defined health software product.

The clinical safety case argument together with its structured evidence shall be identifiable within the risk management file.

NOTE 1: The clinical safety case, as defined in 2.11, comprises an argument based on structured evidence demonstrating the clinical safety of the product. It will develop and evolve through the life cycle of the product (see Annex G).

NOTE 2: For the relationship between the clinical risk management file, clinical safety case, clinical safety case report, clinical risk management close-out report and product life-cycle see Annex G.

5 Clinical risk analysis

NOTE: Clinical risk analysis is normally conducted by a multidisciplinary group including an appropriate registered clinician(s).

5.1 Clinical risk analysis process

Clinical risk analysis shall be performed for the particular health software product as described in 5.2 to 5.4.

The implementation of the planned clinical risk analysis activities and the results of the clinical risk analysis shall be recorded in the clinical risk management file.

NOTE 1: If a clinical risk analysis or other information is available for a similar health software product, it can be used as a starting point provided that changes that have been made are considered, in order to discover if they could introduce significant differences in results. This consideration should be based on a systematic evaluation of the characteristics of the two products, the changes and the ways they can influence the development of various hazardous situations.

NOTE 2: There are many risk analysis techniques but it is not the purpose of this Technical Specification to describe them or to recommend any particular one. ISO 14971 [13] provides guidance on several of the best known techniques.

In addition to the records required in 5.2 to 5.4, the documentation of the conduct and results of the clinical risk analysis shall include at least the following:

- a description and identity of the health software product that was analysed;
- identity of the person(s) who carried out the risk analysis;
- scope and date of the clinical risk analysis.

NOTE 3: The scope of clinical risk analysis can be very broad and “shallow” (as in the earliest, conceptual stages of design and development of a new software product with which the manufacturer has little or no experience) or “deep” (as the design matures and is developed) or the scope can be limited (as for analysing the impact of a change to an existing product for which extensive information already exists in the manufacturing files). Some software might present particularly high potential risks and present considerable challenges; an example might be decision support software (see Annex C).

5.2 Intended use and identification of characteristics related to the clinical safety of the health software product

For the particular health software product being considered, the manufacturer shall document the clinical scope and intended use and any reasonably foreseeable misuse based on a clear understanding of the use environment. The manufacturer shall identify and document those qualitative and quantitative characteristics that could affect the clinical safety of the health software product and, where appropriate, their defined limits.

These documents shall be maintained in the clinical risk management file.

NOTE 1: In this context, misuse is intended to mean incorrect or improper use of the software product. Since incorrect use may well depend on the human/computer interface, consideration of such aspects should include expertise in human factors.

NOTE 2: It is important that the clinical risk management process be firmly based on a detailed understanding of the clinical context into which the health software product is to be introduced and how the product will affect the clinical processes involved. For this reason the clinical risk management process needs to involve clinicians experienced in the field of application (see 4.3).

5.3 Identification of hazards to patients

The manufacturer shall compile documentation on known and foreseeable hazards to patients associated with the health software product in both normal and fault conditions. This documentation shall be maintained in the clinical risk management file.

5.4 Estimation of the clinical risk(s) to a patient for each hazardous situation

Reasonably foreseeable sequences of events that can result in a hazardous situation to a patient shall be considered and the resulting hazardous situation(s) shall be recorded.

For each identified hazardous situation to a patient, the risk(s) in both normal and fault conditions shall be estimated using available information or data and by approaches such as "scenario analysis". Where the likelihood of occurrence of harm to patients cannot be quantified, hazards should still be listed and a reasonably pessimistic qualitative judgement should be used to allow a risk class to be assigned. This allows the manufacturer to focus on reducing clinical risks in the knowledge of their relative seriousness. The results of these activities shall be recorded in the clinical risk management file.

Any system used for qualitative or quantitative categorization of likelihood of occurrence or severity shall be recorded in the risk management file.

NOTE Information or data for risk analysis can be obtained, for example, from:

- published standards;
- scientific technical data;
- field data from similar health software products already in use including published reported incidents;
- usability tests employing typical users;
- clinical evidence;
- results of appropriate research including the use of analytical techniques;
- expert opinion;
- external quality assessment schemes.

6 Clinical risk evaluation

For each identified hazardous situation to a patient, the manufacturer shall decide, using the criteria defined in the clinical risk management plan, whether risk reduction is required. If risk reduction is not required, the requirements given in 7.2 to 7.6 do not apply for this risk (i.e., proceed to 7.7). The results of this clinical risk evaluation and the rationale on which it is based shall be recorded in the clinical risk management file.

NOTE 1: Guidance for deciding on risk acceptability is given in Annex H.

NOTE 2: Risk evaluation will normally be conducted by a multidisciplinary group including an appropriate registered clinician.

7 Clinical risk control

7.1 Clinical risk reduction

When clinical risk reduction is required, clinical risk control activities, as described in 7.2 to 7.7, shall be performed.

7.2 Clinical risk control option analysis

The manufacturer shall identify clinical risk control measure(s) that are appropriate for reducing the clinical risk(s) to an acceptable level. Appropriateness will apply both to the level and to the type of risk and type of health software.

The manufacturer shall use one or more of the following clinical risk control options in the priority order listed:

- inherent safety by design;

- protective measures in the health software product itself or in the manufacturing process;
- product verification, e.g. testing;
- information for patient safety.

The clinical risk control measures selected shall be recorded in the clinical risk management file.

NOTE: Guidance on information for patient safety is provided in Annex I

If, during clinical risk control option analysis, the manufacturer determines that required clinical risk reduction is not practicable, the manufacturer shall conduct a clinical risk/benefit analysis of the residual clinical risk (proceed to 7.5).

7.3 Implementation of clinical risk control measure(s)

The manufacturer shall implement the clinical risk control measure(s) selected in 7.2.

Implementation of each clinical risk control measure shall be verified. This verification shall also be recorded in the clinical risk management file.

The effectiveness of the clinical risk control measure(s) shall be verified and the results shall be recorded in the clinical risk management file.

NOTE: The verification of effectiveness can include validation activities.

7.4 Residual clinical risk evaluation

After the clinical risk control measure(s) are applied, any residual clinical risk shall be evaluated using the criteria defined in the clinical risk management plan. The results of this evaluation shall be recorded in the clinical risk management file.

If the residual clinical risk is judged not acceptable using these criteria, further clinical risk control measures shall be applied (see 7.2).

For residual clinical risks that are judged acceptable, the manufacturer shall decide what information is necessary to include in the accompanying documents in order to disclose fully the residual clinical risk.

NOTE National or regional regulatory requirements may apply and the manufacturer will need to be aware of general legal product liability.

7.5 Clinical risk/benefit analysis

If the residual clinical risk is judged not acceptable using the criteria established in the clinical risk management plan and further clinical risk control is not practicable, the manufacturer may gather and review data and literature to determine if the clinical benefits of the intended use sufficiently outweigh the residual clinical risk. If this evidence does not support the conclusion that the clinical benefits outweigh the residual clinical risk, then the clinical risk remains unacceptable. If the clinical benefits outweigh the residual clinical risk, then proceed to 7.6.

For clinical risks that are demonstrated to be outweighed by the clinical benefits, the manufacturer shall decide which information for clinical safety is necessary to disclose fully the residual clinical risk.

The results of this evaluation shall be recorded in the clinical risk management file.

NOTE In determining whether clinical risks are outweighed by clinical benefits, national or regional regulatory requirements can apply and the manufacturer will need to be aware of general legal product liability.

7.6 Clinical risks arising from clinical risk control measures

The results of the clinical risk control measures shall be reviewed with regard to:

- the introduction of new hazards or hazardous situations to patients;
- whether the estimated clinical risks for previously identified hazardous situations to patients are affected by introduction of the clinical risk control measures.

Any new or increased clinical risks shall be managed in accordance with 5.4 to 7.5.

The results of this review shall be recorded in the clinical risk management file.

7.7 Completeness of clinical risk control

The manufacturer shall be able to demonstrate that the clinical risk(s) from all identifiable hazardous situations to patients have been identified and considered. The results of this activity shall be recorded in the clinical risk management file.

7.8 Evaluation of overall residual clinical risk acceptability

After all clinical risk control measures have been implemented and verified, the manufacturer shall decide if the overall residual clinical risk posed by the health software product is acceptable using the criteria defined in the clinical risk management plan.

If the overall residual clinical risk is judged not acceptable using the criteria established in the clinical risk management plan, the manufacturer may gather and review data and literature on the clinical benefits of the intended use to determine if they outweigh the overall residual clinical risk. If this evidence supports the conclusion that the clinical benefits sufficiently outweigh the overall residual clinical risk, then the overall residual clinical risk can be judged acceptable. Otherwise, the overall residual clinical risk remains unacceptable.

For an overall residual clinical risk that is judged acceptable, the manufacturer shall provide information that is sufficient to fully justify that decision.

The results of the overall residual clinical risk evaluation shall be recorded in the clinical risk management file.

NOTE: In determining whether the overall residual clinical risks are outweighed by clinical benefits, national or regional regulatory requirements can apply and the manufacturer will need to be aware of general legal product liability.

8 Clinical safety case report(s)

The manufacturer shall compile a date-stamped pre-release clinical safety case report. The report shall be available to a customer or regulatory authority.

The clinical safety case report is a primary vehicle for presenting a statement to the customer concerning the clinical safety of the health software product. The content of the clinical safety case report shall provide a summary of knowledge relevant to the customer which has been acquired during the manufacturing process and which relates to the clinical safety of the product including details of the methods and techniques employed by the manufacturer to derive that knowledge and the criteria employed to justify the acceptance of the residual risks.

Thus a clinical safety case report shall, at a minimum, cover the following aspects.

- Introduction and health software identification including:
  - general background;
  - unique identification details including version;
  - detailed product description with details of intended operational environments and any critical constraints.
- Description of general and clinical safety management arrangements.
- Overview of hazard and risk assessment processes including risk evaluation and acceptance criteria covering:
  - identification of the conceptual hazard and risk methodology used;
  - justification of risk acceptance criteria;
  - justification of residual risk criteria.
- Identification and justification of any residual risks.
- Overall clinical safety justification.
- Lifetime management arrangements including:
  - performance monitoring arrangements;
  - incident/adverse event response arrangements;
  - lifetime support arrangements.

Annex J provides further guidance on these aspects.

Where the health software product incorporates a non-health software product such as an OTS or SOUP product or operating system, the clinical safety case report shall describe how the manufacturer has applied this Technical Specification to those products and how subsequent modifications such as upgrades and patches will be dealt with in so far as the manufacturer transfers them to the customer/user.

Whenever any aspect of the clinical risk management process for the product is reviewed the results shall be reflected in an updated clinical safety case report.

It is permissible for the required content of the safety case report to be contained in the manufacturer's accompanying documents.

The clinical safety case report shall be included in the clinical risk management file.

NOTE 1: The clinical safety case is an argument based on evolving experience and documentation but takes definitive forms at 'gateways' between the stages of the product life-cycle (see Figure G.1). The most appropriate clinical safety case report for meeting the customer's requirements is a report at the “Application/system delivery” point of the life cycle i.e. pre-release. However, a contract with a customer might require a safety case report at other points in the life cycle.

The decision as to which other point(s) in the product life-cycle a clinical safety case report will be necessary will depend on the contract with the customer and thus such other reports are not a requirement of this Technical Specification. For example where the manufacturer is responsible for deployment a report at the “Deployment” point of the life cycle might be required by the customer. If the customer is involved in specifying the product, the customer may require a clinical safety case report at the “Concept” and “Product” points of the product's life cycle. Where the customer has contracted a manufacturer to manage the whole life cycle of the product, the customer may require a clinical safety case report at any or all points of the product life-cycle including the “Operational” and “Decommissioning” points.

NOTE 2: For the relationship between clinical risk management file, clinical safety case, clinical safety case report, stage report and product life-cycle, see Annex G.

9 Stage reports and pre-release clinical risk management process review

The manufacturer shall undertake a review at each defined stage of the product's life cycle to ensure that all that needs to be done according to the risk management plan, has been done. The results of the review shall be recorded in a stage report which shall be signed off by top management before proceeding to the next stage.

Prior to release for distribution or deployment of the health software product, the manufacturer shall carry out a particularly rigorous, in-depth review of the clinical risk management process. This review shall at least ensure that:

- the clinical risk management plan has been appropriately implemented and the outcomes have been captured;
- verification that the agreed controls have been effectively implemented;
- the overall residual clinical risk is acceptable using the criteria defined in the clinical risk management plan;
- appropriate methods are in place to obtain relevant post-deployment information;
- a sufficient and accurate clinical safety report has been produced.

The results of this review shall be recorded as the pre-release stage report which shall comprise a sign-off of all processes before product distribution or deployment. The formal sign-off shall be undertaken by top management.

All stage reports shall be included in the clinical risk management file.

The responsibility for the pre-release review should be assigned in the clinical risk management plan to persons having the appropriate authority to recommend the release of the software for deployment (see 4.2).

NOTE 1: A pre-release stage report should not be confused with a clinical safety case report. The latter is a document specifically intended for communication, e.g. to the customer/user, and may be produced at any point in the product's life cycle. The pre-release stage report is a document to demonstrate that all processes have been satisfactorily undertaken (including the creation of a clinical safety case and clinical safety case reports) before the product is released for distribution or deployment.

NOTE 2: For the relationship between a clinical risk management file, clinical safety case, clinical safety case reports, stage reports and product life-cycle see Annex G.

10 Post-deployment monitoring

The manufacturer shall establish, document and maintain a system to collect and review information about the clinical safety performance of the health software product or similar products in the post-deployment phase.

When establishing a system to collect and review information about the software product, the manufacturer should consider, among other things:

- the mechanisms by which information generated by the user or those accountable for the deployment, use and maintenance of the health software product, is collected and processed and any agreements with users on the mechanism for reporting;
- new or revised standards.

The system should also collect and review publicly available information about similar health software products on the market.

This information shall be evaluated for possible relevance to clinical safety, especially the following:

- if previously unrecognised hazards or hazardous situations to patients are present or
- if the estimated clinical risk(s) arising from a hazardous situation to patients appear incorrect or are no longer acceptable.

If any of the above conditions occur:

- a review of the clinical risk management file for the health software product shall be conducted; if there is a potential that the residual clinical risk(s) or its acceptability has changed, the impact on previously implemented clinical risk control measures shall be evaluated;
- the impact on previously implemented clinical risk management activities shall be evaluated and shall be fed back as input to the clinical risk management process;
- the results of this evaluation shall be recorded in the clinical risk management file.

The manufacturer shall have in place a procedure for issuing an “alert” to all customers of a product if post-deployment monitoring reveals a significant risk to patients.

NOTE: Some aspects of post-deployment monitoring may be the subject of some national regulations. In such cases, additional measures might be required.

11 Product modification

Health software products are often modified through release of amended versions, up-dates or “patches”.

Whenever the product is modified, a suitable and sufficient clinical risk analysis, commensurate with the scale and extent of the modification (itself established by risk analysis), shall be undertaken to establish what, if any, new clinical risks have been introduced. An audit trail of all versions and patches released to the market so as to provide traceability in the event of a hazard alert shall be maintained. Where the health software product includes a non-health software product such as an OTS or SOUP product or operating system, modification of the health software product shall include any modification to the non-health/OTS/SOUP product or operating system.

The results shall be recorded in the clinical risk management file and the clinical safety case amended as appropriate.

NOTE: The extent of the repeat clinical risk analysis will depend on the extent and the nature of the product modification. However, even apparently minor modifications can result in substantial clinical risks and thus, whatever the extent of the clinical risk analysis undertaken, it will need to be executed formally, rigorously and with due process.

12 Regular clinical risk management process review and maintenance

The means to be adopted for the maintenance of the clinical risk management process shall be documented and shall be included in the clinical risk management file.

The risk management process shall be formally reviewed regularly at least once a year.

13 Compliance with this Technical Specification

Any software product that is regulated as a medical device and whose manufacture is in compliance with ISO 14971, can be considered as in compliance with this Technical Specification with the addition of 4.6, Clause 8 and Clause 11.

Where a manufacturer buys health software from an external source, e.g. for incorporation into, or as a support to, his own product, the manufactures shall ensure that the bought-in health software complies with this Technical Specification.

NOTE: The potential that health software products have for causing harm to patients varies considerably across the supplier domain. EN TS 15260 [10] describes a means for classifying health software according to the risks it may present to patients and application of that TS, or other classification systems, will assist in formally assessing the maximum extent to which a product presents a patient safety risk. For products that have been assessed in this way and found to present little, if any, risk, the application of this Technical Specification may at first sight seem burdensome. However this need not be so since the risk management file and the safety case will necessarily be slim, the safety case report short and the organizational structures underpinning compliance with this Technical Specification will evidently depend on the maximum risk that a product can present to a patient, i.e. it may be simple and small for low risk products. The matter of overriding importance is that, no matter what the health software product, a hazard and risk analysis should be undertaken in a formal way and the results documented with a summary available to any customer. These basic processes represent the underlying substance of this Technical Specification. Even non-complex software that might at first sight seem to be innocuous, may prove less so when formally analysed. Without analysis no valid safety claim can be made even though in some cases the analysis may be relatively simple and straightforward. It will be for a manufacturer to demonstrate that a product is of low or negligible risk to patients, by using a respected methodology. If that can be demonstrated satisfactorily, this note recognises that the manufacturer can justifiably present a case that simplification of the application of the processes required in this Technical Specification, the extent of the resource devoted to them and the level of complexity and content of documentation is appropriate to that low/negligible risk.

Annex A (informative) Examples of potential harm presented by health software

A.1 Background

The increasing introduction of software into the health sector can give rise to a variety of hazardous incidents.

The following is a selection of fairly typical and recent high profile incidents that have actually occurred in service, presented in no particular order. All represent significant, high profile hazards.

A.2 GP prescribing decision support

In 2004 the four most commonly used GP systems in the UK were subjected to eighteen potentially serious, realistic scenarios including an aspirin prescription for an eight year old, penicillin for a patient with penicillin allergy and a combined oral contraceptive for a patient with a history of deep vein thrombosis. Using dummy records, all eighteen scenarios failed to produce appropriate alerts by all of the systems, most of the time. The best score was a system that flagged up seven appropriate alerts.

A.3 Inadvertent accidental prescribing of dangerous drugs (such as methotrexate)

This incident occurred when a user of a GP system attempted to issue two repeat items. The items were highlighted and instead of the “issue selected repeats” button, the “prescribe acute issues from the formulary” button was pressed. This brought up the formulary dialogue which contained the high risk items. Either the “issue” button was then pressed or the particular items were double clicked. When the warning messages came up, they were all ignored and “proceed” and “issue” selected. The user chose the first item presented on the formulary list, which just so happened to be methotrexate injection.

In this particular case, it was determined that patient risk was minimal as the treatment was rarely used in primary care and would, in practice, be rejected by the pharmacist. To preclude any recurrence of the problem, access to the high risk formulary was removed from the formulary part of the acute drug issue dialogue.

A.4 Incorrect patient details retrieved from radiology information system

This incident arose from the fact that Medical Reference Numbers (MRNs) are usually prefixed by an alpha code. Some hospitals however do not use these prefixes and identical MRNs can be generated. This gave rise to the creation of “shared” MRNs and subsequent confusion of records in the central datastore when a retrieval key is the Medical Record Number. Four specific instances were found where a patient number had been entered in the Radiology Information System and incorrect patient details had been retrieved.

A.5 CT and MRI images could not be seen after being moved to PACS

Prior to the introduction of the Picture Archiving and Communication System (PACS) it had been common practice to wire Computed Tomography (CT) and Magnetic Resonance Imaging (MRI) images between paediatricians and a regional paediatric tertiary referral centre. After the installation of a PACS this was found to be no longer possible, and images were sent on CD via taxi. In emergency cases the images were being e-mailed. This is an issue related to the establishment of clinical data sharing policy and protocols. Because these were omitted from original commercial agreements the resulting delays gave rise to real operational difficulties and potential for patient harm.

A.6 Drug mapping error

Sodium valproate 200 mg slow release was incorrectly mapped to sodium valproate 200 mg. These are anti-epilepsy drugs and thus the implications for patient safety could be significant. This particular incident was one of many related to drug mapping.

An initial investigation indicated that 35 prescriptions had been generated using the incorrect map. Corrective action included contacting the relevant primary care practices and the supplier correcting the mapping process to ensure no further incorrect prescriptions were generated.

A.7 Pre-natal screening

The ages of women who had undergone pre-natal screening were wrongly computed by a health software system. As a result 150 women were wrongly notified that they were at no risk. Of these, four gave birth to Down's syndrome babies and two others made belated decisions to have abortions.

A.8 Radiotherapy errors

Over a period of ten years a computer programming error resulted in nearly 1 000 patients being given radiotherapy that was between 10 % and 30 % below that required. This is one of a number of errors in programming in this field. The Chief Medical Officer for England devoted a chapter to such errors in his 2006 Annual Report [35]. He highlighted three radiotherapy centres where there had been deaths, injury or inadequate treatment of patients due to inaccurate transfer of data between software systems and an unidentified risk in computerized adjustments of dosage. These errors had been unrecognised for considerable periods therefore affecting many patients.

A.9 Patient identification

A student died of meningitis because of a misspelling of her name and inadequacy in computer use. The student was admitted and a blood test proved negative for meningitis. The following day another blood test was taken and filed on a new computer entry but the letter “p” was missed in the spelling of the name. When a doctor looked up results they were presented with only the first negative test results because of the misspelling. If the second result had been seen it would have triggered further investigations and probable diagnosis of meningitis.

The investigating panel concluded that problems with the health software system had been greater than first thought and in this case there was a combination of a misspelled name and the doctor not being able to use the computer system properly.

A.10 Ambulance system

During installation of a new ambulance dispatch system, an operator switched off his visual display unit by pressing a wrong button by mistake. This meant that calls coming in to the control room were not allocated to ambulances. Because the system was being implemented in stages, an alarm which should have alerted staff to the problem was not working. This may have contributed to the death of a patient.

A.11 Slack security

A nurse was jailed for gaining unauthorized access to a hospital's computer system and prescribing potentially lethal drugs to a 9-year-old suspected meningitis patient. The nurse had used the system on other occasions to prescribe drugs. Access was gained because five months earlier the nurse memorized the PIN number of a locum doctor who was having difficulty logging on to the system. Investigations demonstrated that the hospital's software system was subject to poor security measures.

Annex B (informative) **Conclusions of the CEN/TR measures for ensuring patient safety of health software**

If health software products are to be regulated or controlled formally or informally at national, regional or local levels, the controls will need to be founded on standards. EN TR 15640 [11] considered the standards needed and their nature. The conclusions are as follows.

a) 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. EN TS 15620:2006 [10] is deemed the most appropriate for such classification subject to its validation as a Technical Specification (particularly Table 4).

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

c) A standard on the minimum information required for documentation of the characteristics of health software products could be advantageous particularly regarding those characteristics which are significant for interworking and interoperability. The standard for medical devices EN 1041 [22] should be reviewed to assess whether there is a need for a standard on general labelling of health software products.

d) 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 the latter context ISO 14155 [23] should be reviewed for its applicability.

e) Incident reporting may be regarded as necessary in which case a standard on electronic reporting of adverse incidents should be considered.

f) 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 [24]. 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 [25] 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 [26] and its associated guide ISO/TR 14969 [27].

g) 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 references [28] [29], 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.

h) If risk management is to be part of the requirements for ensuring the safety of health software products then a new standard, consistent at a high level with the results of ISO/TMB WG [12], ISO 14971 [13], IEC 61508-3 [14] and IEC 61508-5 [15], is required specifically for health software products. That standard should embody the concepts in GHTF/SG3/NI5R8 [16] and build on the experience of the use of CRAMM [17] with ISO 17799 (now numbered ISO 27001 [18]). The new standard should be backed by an implementation guide specific to health software products.

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

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

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

Annex C (informative) **Decision support software**

C.1 Background

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 support, rather than clinical delivery, 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.

Systems incorporating decision support can reduce clinical errors and improve clinical practice but they also carry the potential for harm. Whereas this may be the result of unquestioning and/or non-professional use it may lie in the system design such as:

- poor evidence base;
- failure of logic to properly represent 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 deficiencies may be invisible to the user, particularly the reliance that may be placed on the clinical evidence underpinning decision support systems. Unless evidence is sound and kept up-to-date with clinical knowledge and practice, patient safety may compromised. Of course potential risks will depend on the decision support system, examples being:

- medical text books (map of medicine), type where the decision support is in navigating the data;
- alerts and warnings on prescribing systems;
- paediatric dosage calculators;
- full blown bowel cancer treatment regime recommendations.

References [38] and [39] describe the kinds of unintended consequences related to the implementation of computerized provider order entry in decision support systems.

Thus some special consideration of decision support systems is warranted as indicated in Clause C.2.

C.2 Risk management for decision support software

Application of hazard and risk identification to decision support software needs to be particularly rigorous and involve clinical experts in the subject area who will need to be able to understand the algorithms and the clinical evidence which may underpin them. Rigorous reviews at regular intervals will be necessary to ensure the evidence and algorithms are kept up-to–date and that whenever new clinical evidence emerges, and is incorporated into new releases, no new risks arise.

A particularly important stage for rigour will be in original design of algorithms etc. and associated risk avoidance and mitigation. These aspects of risk management will merge with formal design control methodologies. See Clause C.3.

C.3 Design control

Design control is an important part of quality management and this was considered in EN TR 15640 [11], the conclusions of which are given in Annex B. CEN/TC 251 and ISO/TC 215 considered these conclusions in a document – see reference [19], the most relevant part of which reads:

"Conclusions 6, 7 and 8 on quality systems, design control and risk management are interlinked in that quality systems will usually encompass both design control and risk management. It might therefore be possible to bring all three conclusions together into one standard on quality systems. However, experience with medical devices demonstrates that the preferred solution would be three separate standards for health software products. They would need to be consistent with each other and consistent with the standards that apply to medical devices. Of these three standards it is proposed that the priority should be risk management."

This Technical Specification addresses the risk management aspect of quality management. It does not address design control except in so far as it is part of risk management. Whether Conclusion 6 (regarding quality management) and/or Conclusion 7 (regarding design control), as reproduced in Annex B, are pursued will be for CEN/TC 251 and ISO/TC 215 to decide. However it should be noted that Conclusion 7 highlights decision support software as follows:

"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 – references [28] [29], 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."

Although this Technical Specification does not address design control, the latter and risk management often interact and merge at the design stage. Thus design control and risk avoidance and mitigation with decision support software may employ similar processes such as:

- formal methods for design specification;
- mathematical proving of algorithms;
- rigorous proving of inference engine using panels of recognised experts;
- structured clinical validation against evidence and peer review;
- clinical trials;
- dissimilarity (independently building alternative algorithms to run in parallel) with comparisons for reasonableness of results.

Annex D (informative) **Rationale for this Technical Specification**

D.1 Background

As stated in the Introduction, in many countries the safety of medicines and of medical devices is ensured through legal measures. Some software is covered by such medical device legislative controls. However there is other software applied to health which is not usually covered or is encompassed in a less than clear manner or is currently not a primary focus of some regulatory bodies. These matters are considered in EN TR 15640 [11] and the argumentation is not therefore repeated here. Its eleven conclusions are reproduced in Annex B.

Conclusion 8 reads:

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

- A new standard, consistent at a high level with the results of ISO/TMB WG [12], ISO 14971 [13], ISO 61508-3 [14] and ISO 61508-5 [15], is required specifically for health software products. That standard should embody the concepts in GHTF/SG3/NI5R8 [16] and build on the experience of the use of CRAMM [17] with ISO 17799 (now numbered ISO 27001 [18]).
- The new standard should be backed by an implementation guide specific to health software products."

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

D.2 Utilization of this Technical Specification

There are a variety of means under which standards will be utilized including:

- user pressure;
- purchasing contracts;
- local, national or regional regulations.

They may of course be adopted voluntarily by manufacturers.

This Technical Specification makes no presumption about its mode of enforcement.

D.3 Relationship with ISO 14971

The relationship of this Technical Specification with ISO 14971 [13] is outlined in the Introduction. For reasons stated there, this Technical Specification takes as its baseline ISO 14971. As far as practicable the layout and requirements of the main text of ISO 14971 have been retained. However most of the annexes to ISO 14971 are clearly not applicable to health software and have therefore been replaced or amended as appropriate.

The main differences are the additions of the requirements:

- to compile a clinical safety case (see 4.6);
- to make available a clinical safety case report to a customer or regulatory authority (Clause 8);
- to undertake necessary steps to identify any differences in risk when a product is modified (Clause 11).

Whilst there are also some wording differences these do not represent substantial changes: this justifies the paragraph from Clause 13 reading:

"Any software product that is regulated as a medical device and whose manufacture is in compliance with ISO 14971, can be considered as in compliance with this Technical Specification with the addition of 4.6, Clause 8 and Clause 11."

D.4 Link between the manufacturer and user domains — The clinical safety case report

This Technical Specification is concerned with the manufacturer domain. However a manufacturer's health software product will be deployed in a user domain. A user will need:

- to be assured that the manufacturer has satisfactorily applied clinical risk management to the product which has been supplied;
- to have information on any clinical risks associated with the product and how they have been addressed with, in particular, details of any residual clinical risks.

It is for this purpose that this Technical Specification requires a manufacturer to develop and maintain a clinical safety case and to make available to the customer a clinical safety case report(s) (see 4.6, Clause 8, D.5.8 and Annex J). The clinical safety case report(s), based on the clinical safety case, provide(s) the clinical risk management interface between manufacture and customer.

CEN/TC 251 and ISO/TC 215 under the Vienna agreement have prepared ISO/TR 29322 [35]. This deals with risk management in the user domain, an input to which the clinical safety case reports from manufacturers of the products are deployed in that domain.

D.5 Rationale for requirements in particular clauses and subclauses

D.5.1 Scope

NOTE: The scope is intended to cover health software products which are not covered by medical device regulations.

It is acknowledged that, on the boundary, there are health software products that are encompassed by medical device regulations in some countries but not in others. This matter is considered in detail in EN TR 15640 [11] and should be referred to for argumentation and analysis.

Risks can be introduced throughout product life-cycle, and risks that become apparent at one point in the life cycle can be managed by action taken at a completely different point in the life-cycle. The extent to which the manufacturer is involved or responsible for different aspects of product life-cycle will depend on the scope of the contract with the customer: hence the need for the NOTE under D.5.2.

D.5.2 Terms and definitions

Existing international definitions have been used wherever possible with many having been taken from ISO 14971. Modifications are typically for the purpose of making clear the clinical nature of this Technical Specification.

The definition of health software product (see 2.17) is for the purpose of this document only. In that respect the note is particularly important. It reads:

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

The definition of “intended use” (see 2.18) includes “use of …. in accordance with … information provided by the manufacturer”. The Note under 2.18 reads “Information provided by the manufacturer includes information relevant to misuse as determined by the risk management processes laid down in this Technical Specification”. The purpose of the Note is to ensure that the manufacturer cannot escape responsibility for addressing possible risks which the manufacturer has identified as arising from foreseeable misuse in the clinical risk management process.

The definition of “manufacturer” (see 2.20) is qualified by the Note reading “A manufacturer may be involved in part of or the whole of the software life-cycle including deployment, use and decommissioning of the software according to the contractual scope with the customer.” Deployment, use and decommissioning are not usually associated with manufacture and the note is an alert that the scope of the risk management this Technical Specification addresses will cover those aspects if the contract with a customer includes them.

The definition of a medical device (see 2.21) is that of the GHTF. However, as discussed in EN TR 15640 [11], the definition varies globally with respect to software. The Note under 2.21 is therefore particularly important.

D.5.3 General requirements for effective clinical risk management

D.5.3.1 Clinical risk management process

Subclause 4.1 requires the manufacturer to establish a clinical risk management process as part of the design of a health software product. This is required so that the manufacturer can systematically ensure that the required elements are in the process. Clinical risk analysis, risk evaluation and risk control are commonly recognised as essential parts of risk management. In addition to these elements, the Technical Specification emphasizes that the clinical risk management process does not end with the design and production of a health software product, but continues on into the post-production phase. Therefore, the specification and gathering of post deployment clinical safety relevant information is identified as a required part of the clinical risk management process.

The clinical risk management system may be part of a wider clinical management system which itself may be part of the manufacturer's quality management system. Whereas it is not within the scope of this Technical Specification to require a manufacturer to have a clinical management system or a quality management system, this is recognised as good practice. It is further noted that it would be difficult to fulfil the aims of this standard without a quality management system being in place (see also conclusion 6 in Annex B).

D.5.3.2 Management responsibilities

The commitment of top management is critical for an effective clinical risk management process. Thus top management will need to take responsibility for overall guidance of the risk management process, to ensure it is independent. In particular it should be noted that:

- in the absence of adequate resources, risk management activities may be ineffective and put the manufacturer at risk of not complying with legal responsibilities in terms of product liability and other national legal responsibilities, even if complying with the letter of the other requirements of this Technical Specification;
- clinical risk management is a specialized discipline and requires the involvement of individuals trained in risk management techniques and software system engineering; it also requires clinical input from clinicians who are knowledgeable and experienced in the environment in which the product is to be used and in the clinical processes involved;
- because this Technical Specification does not define acceptable clinical risk levels, top management are required to establish a policy on how acceptable clinical risks will be determined and to ensure they are in line with any national requirements and legal product liability;
- clinical risk management is an evolving process and periodic review of risk management activities is needed to ascertain whether they are being carried out correctly, to rectify any weaknesses, to implement improvements, and to adapt to changes.

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

D.5.3.3 Competencies of personnel

It is most important to get people with the expertise necessary to perform clinical risk management tasks. The risk management process requires people with expertise in areas such as:

- how the health software product is compiled;
- how the health software product works;
- how the health software product is produced;
- how the health software product is actually used;

- how to apply the clinical risk management process.

In general, this will require several representatives from various functions or disciplines, each contributing their specialist knowledge. Clinical knowledge and experience relevant to the field of application of the product will be particularly important and thus the involvement of appropriate clinicians is essential. Normally this will include an appropriate registered clinician. A balance of skills should be demonstrated in the structure of a working clinical safety team and the process should clearly define roles and responsibilities to ensure that the right skills are suitably involved in significant decisions etc.

D.5.3.4 Clinical risk management plan

A clinical risk management plan is required because:

- an organized approach is essential for good clinical risk management;
- the plan provides the roadmap for clinical risk management;
- the plan encourages objectivity and helps prevent essential elements being forgotten.

The elements listed (see 4.4) are the minimum necessary. Annex E provides guidance on the clinical risk management plan.

D.5.3.5 Clinical risk management file

This Technical Specification uses this term to signify where the manufacturer can place or find the locations of all the records applicable to clinical risk management. This facilitates the clinical risk management process and enables more efficient auditing of this Technical Specification where that is necessary. Traceability is necessary to demonstrate that the clinical risk management process has been applied to each identified hazard to patients.

Completeness is very important in clinical risk management. An incomplete task can mean that an identified hazard to patients is not controlled and harm to a patient can be the consequence. The problem can result from incompleteness at any stage of clinical risk management, e.g. unidentified hazards, clinical risks not assessed, unspecified clinical risk control measures, clinical risk control measures not implemented or clinical risk control measures that prove ineffective. Traceability is needed to provide a record from cause to solution that can be used to demonstrate that the proper process has been completed against each issue that needs to be addressed.

D.5.4 Clinical safety case

If the safety of a health software product is to be ensured, then a structured and disciplined approach to assessing risk is necessary and that approach needs to be based on an argument backed by structured evidence and documentation. The safety case comprises that argument and evidence. Safety cases have become common practice in many industry and public service sectors where they have been well tried and tested. They are applied wherever there is a need to demonstrate either compliance with legislative requirements, or a need to explain/prove that an effective process exists, and that sufficient deliberation is being applied to the management of safety.

The clinical safety case is an argument, supported by a structured body of evidence and documentation in the clinical risk management file, which provides a compelling, comprehensible and valid case that a system is, as far as the clinical risk management process can ascertain, free from unacceptable clinical risk for its intended use. The argument and evidence is the most important aspect. The latter will evolve with the product life-cycle and the argument should become more solid with the progress of testing, deployment and experience in use.

This requirement is additional to ISO 14971 and builds on experience in other fields (see the UK Defence standard “Safety Management Requirements for Defence Systems” Parts 1 and 2 [32] of which Part 2 provides guidance on the safety case).

D.5.5 Clinical risk analysis

D.5.5.1 Clinical risk analysis process

Note 1 under 5.1 describes how to deal with the availability of a clinical risk analysis for a similar health software product. The note informs users of this Technical Specification that when adequate information already exists it can and should be applied to save time, effort and other resources. Users of this Technical Specification need to be careful, however, to systematically assess the previous work for applicability to the current clinical risk analysis.

Note that details required by the three indents in 5.1 form the basic minimum data set for ensuring traceability and are important for management reviews and for subsequent audits. The requirement in the first indent also helps to clarify what is in the scope of the analysis and to verify completeness.

D.5.5.2 Intended use and identification of characteristics related to the clinical safety of the health software product

This step forces the manufacturer to think about all the characteristics that could affect clinical safety of the health software product. The manufacturer should also consider the intended user(s) of the health software product, e.g. whether a lay user or a trained medical professional will use the health software product. This analysis should consider that health software products may be used in situations other than those intended by the manufacturer and in situations other than those foreseen when a health software product is first conceived. It is important that the manufacturer tries to look into the future to see the hazards to patients due to potential uses (and misuses) of their health software product. For this analysis expert clinical input will be essential.

D.5.5.3 Identification of hazards to patients

This step requires that the manufacturer be systematic in the identification of anticipated hazards to patients in both normal and fault conditions.

D.5.5.4 Estimation of the risk(s) to a patient for each hazardous situation

A clinical risk can only be assessed and managed once a hazardous situation has been identified.

Documenting the reasonably foreseeable sequences of events that can influence the significance of a hazard and thus transform the hazard into a significant risk allows this to be done systematically.

This is a critical step in clinical risk analysis. The difficulty of this step is that estimation of clinical risk is different for every hazardous situation that is under investigation as well as for every health software product.

Therefore, this subclause was written generically. Because hazards can occur both when the health software product functions normally and when it malfunctions, both should be looked at closely. In practice, the components of risk, likelihood and consequence should be analysed separately. When a manufacturer uses a systematic way of categorizing the severity levels or likelihood of occurrence of harm levels, the categorization scheme should be defined and recorded in the clinical risk management file. This enables the manufacturer to treat equivalent clinical risks consistently and serves as evidence that the manufacturer has done so, having sought out whatever constitutes the “realistic worst cases”.

Some hazardous situations to patients occur because of systematic faults or sequences of events and this dominates with software. There is no consensus on how to calculate the likelihood of a systematic fault.

Where the likelihood of occurrence of harm to patients cannot be quantified, hazards should still be listed and a reasonably pessimistic qualitative judgement should be used to allow a risk class to be assigned. This allows the manufacturer to focus on reducing clinical risks in the knowledge of their relative seriousness.

Good quantitative data is very rarely available. The suggestion that estimation of clinical risk should be done only in a quantitative way has therefore been avoided. However, expert, qualitative opinion is an acceptable and very effective technique to broadly quantify risks in the absence of valid empirical data, assuming a suitable set of experts can be found and a consensus obtained.

D.5.6 Clinical risk evaluation

Decisions shall be made about the acceptability of each clinical risk using the acceptability criteria defined in the clinical risk management plan. Annex H provides some advice for this difficult area in which the criteria needs to be transparent to customers and others such as regulators and where the criteria will need the input not only of appropriate, experienced clinicians but also will need to take account of any national guidance or requirements and general responsibilities related to legal product liability requirements.

D.5.7 Clinical risk control

D.5.7.1 Clinical risk reduction

It is intended that steps 7.2 to 7.7 make up a logical sequence of tasks. This systematic approach is important since it ensures that relevant information is available when required.

D.5.7.2 Clinical risk control option analysis

Often there will be more than one way to reduce a clinical risk. The three mechanisms are listed in priority order:

- inherent safety by design;
- protective measures in the health software product itself or in the manufacturing process;
- information for safety.

The priority order is important.

It is recognised that one possible result of the clinical risk control option analysis could be that there is no practicable way of reducing the clinical risk to acceptable levels according to the pre-established criteria for clinical risk acceptability. In this case, a clinical risk/benefit analysis can be carried out as described in 7.5 in order to determine whether the clinical benefit of the health software product to the patient outweighs the residual clinical risk. This option is included at this point to make sure that every effort was made to reduce clinical risks to the pre-established acceptable levels.

D.5.7.3 Implementation of clinical risk control measures

Two distinct verifications are included. The first verification is required to make sure that the clinical risk control measure has been implemented in the final design. The second verification is required to ensure that the measure as implemented actually operates and successfully reduces the clinical risk. In some instances, a validation study can be used for verifying the effectiveness of the clinical risk control measure.

D.5.7.4 Residual clinical risk evaluation

A check was introduced here to determine whether the implemented measures have made the clinical risk acceptable. If the clinical risk is not less than the criteria established in the clinical risk management plan, manufacturers are required to assess additional clinical risk control measures. This iterative procedure should be continued until the clinical risk is reduced to within the acceptable levels established in the clinical risk management plan.

Customers should be provided with relevant information on residual clinical risks so that the customer can make informed decisions. Whereas it is the manufacturer's decision as to what and how much information on residual clinical risk needs to be provided in order to reveal fully the residual clinical risks, this needs to be done in the light of any national guidance and the manufacturer's legal product liability.

D.5.7.5 Clinical risk/benefit analysis

There may be some occasions where the clinical risk of a health software product is greater than the manufacturer's criterion for acceptable clinical risk. This subclause enables the manufacturer to provide a high-risk health software product for which they have carried out a careful clinical evaluation and can show that the clinical benefit of the health software product outweighs the risk. It is essential for customers to be informed of significant residual clinical risks and resulting clinical benefits so that informed decisions can be made (see Annex I).

Whereas it is the manufacturer's decision as to what and how much information on the risk benefit analysis needs to be provided in order to reveal fully the clinical risks, this needs to be done in the light of any national guidance and the manufacturer's legal product liability.

D.5.7.6 Clinical risks arising from clinical risk control measures

This subclause recognises that clinical risk control measures alone or in combination might introduce a new and sometimes quite different hazard to patients and that measures introduced to reduce one clinical risk might increase another clinical risk.

D.5.7.7 Completeness of clinical risk control

At this stage, the clinical risk of all the hazards to patients should have been evaluated. This check is introduced to ensure that no hazards to patients were left out in the intricacies of a complex clinical risk analysis.

D.5.7.8 Evaluation of overall residual clinical risk acceptability

During the process defined by Clauses 5 to 7, manufacturers identify hazards to patients, evaluate the clinical risks and implement clinical risk control measures in their design one at a time. This is the point where the manufacturer has to step back, consider the combined impact of the individual residual clinical risks, and make a decision as to whether to proceed with the health software product. It is possible that the overall residual clinical risk can exceed the manufacturer's criteria for acceptable clinical risk, even though individual residual clinical risks do not. This is particularly true for complex systems and health software products with a large number of clinical risks. Even if the overall residual clinical risk exceeds the criterion in the risk management plan, the manufacturer has an opportunity to do an overall clinical risk/benefit evaluation to determine whether a high-risk, but highly beneficial, health software product should be marketed. It is essential for customers to be fully informed of significant overall clinical residual risks. Thus, manufacturers are required to include pertinent information in the accompanying documents and clinical safety case (see Clause 8 and Annexes I and J).

Whereas it is the manufacturer's decision as to what and how much information on the risk benefit analysis needs to be provided in order to reveal fully the clinical risks, this needs to be done in the light of any national guidance and the manufacturer's legal product liability.

D.5.8 Clinical safety case report

It is essential that the manufacturer be able to demonstrate, in an argued and structured manner based, as far as possible, on evidence that all that is necessary has been done to ensure the safety of a health software product. It will be necessary, if required, for the manufacturer to be able to demonstrate this to customers and perhaps to others such as regulators. The clinical safety case is the argument per se plus evidence and is the most important part of the clinical risk management file. The clinical safety report is the means for communicating the summary of the argument and evidence of the clinical safety case at a defined point in the health software's life cycle. The contents of a clinical safety case need to be sufficient and these are detailed in Clause 8 and Annex J.

The clinical safety case report is of particular value to the customer. It provides the essential starting point for the customer to conduct his own risk management processes in deploying a product and for ensuring interoperability with other products from other manufacturers. This aspect is further discussed in ISO/TR 29322 [35].

D.5.9 Stage reports and pre-release clinical risk management process review

Stage reviews are an important part of the clinical risk management process and thus it is important that they are signed off by top management.

The pre-release stage report is a particularly important and essential element of the process and a crucial part of the risk management file. It is intended to be a summary of the review of the final results of the risk management process for the team involved and for top management. The report serves as the high level document that provides evidence that the manufacturer has ensured that the risk management plan has been satisfactorily fulfilled and that results confirm that the required objective has been achieved before the product is released for distribution or deployment. It is not just a summary of documentation but a summary of the review. It is the review that is the important part of this requirement and it needs to encompass every aspect of the risk management plan.

D.5.10 Post-deployment monitoring

It cannot be emphasized too often that clinical risk management does not stop when a health software product goes into use. Clinical risk management often begins with an idea with no physical manifestation of the health software product. Clinical risk estimates can, and should, be refined throughout the design process and made more accurate when a functioning prototype is built. Information for use in clinical risk management can come from any source including production or quality records. However, no amount of modelling can substitute for actual user experience of a health software product. Therefore, the manufacturers should, wherever possible, monitor and collect empirical evidence that is relevant to clinical risk estimates and, therefore, the clinical risk management decisions that have been made during the development of the software. Arrangements should be made with customers for such reporting. With post-deployment information, the clinical risk management process becomes an iterative closed-loop process. Post-deployment monitoring will need to take account of any national regulations or other reporting requirements.

D.5.11 Product modification

It is a characteristic of software that it is often modified in various ways e.g. as updates or remedial patches.

Such modifications to health software may result in the introduction of new hazards or changes to existing hazards and controls. These also need to be subjected to risk management applied in the formal manner required by this Technical Specification.

D.5.12 Regular clinical risk management process review and maintenance

The clinical risk management process itself should not be allowed to become inflexible or outdated.

Experience will reveal weaknesses and new risk management techniques will emerge perhaps backed by standards. Thus experience should be fed back into a process for both maintenance and enhancement. A formal review of the process itself needs to be conducted at regular intervals and once a year is regarded as a minimum.

D.5.13 Compliance with this Technical Specification

The requirements of this Technical Specification are substantially the same as those of ISO 14971 with the exception of 4.6, Clause 8 and Clause 11. Software which is regulated as a medical device and which complies with ISO 14971 can therefore be regarded as in compliance with this Technical Specification provided it also complies with 4.6 and Clauses 8 and 11. Clause 13 of this Technical Specification endeavours to make that clear.

Manufacturers often buy software products from other suppliers to support, or incorporate into, their own product. The whole is often marketed as the manufacturer's product. It is important in this case that the manufacturer takes responsibility for the safety of the whole i.e. takes whatever steps are necessary to ensure that the bought-in product(s) comply with this Technical Specification.

Annex E (informative) **Clinical risk management plan**

E.1 Introduction

The clinical risk management plan can be a separate document or it can be integrated within other documentation, e.g. the clinical safety management system which in turn may be part of the quality management system or the enterprise risk management system. It can be self-contained or it can reference other documents to fulfil the requirements described in 4.4.

The makeup and level of detail for the plan should be commensurate with the level of clinical risk associated with the health software product. The requirements identified in 4.4 are the minimum requirements for a clinical risk management plan. Manufacturers can include other items such as time-schedule, risk analysis tools, or a rationale for the choice of specific clinical risk acceptability criteria. The makeup and level of detail for the plan should be commensurate with the level of clinical risk associated with the health software product.

E.2 The scope of the plan, identifying and describing the health software product, the context in which it will be used and the life-cycle phases for which each element of the plan is applicable

All elements of the clinical risk management process should be mapped to the manufacturer's defined product life-cycle. Some of the elements of the clinical risk management process will occur during the phases of the manufacturer's established product realization process such as design and development control. The remaining elements will occur during the other life-cycle phases through to product decommissioning in so far as the manufacturer is involved in these phases. The clinical risk management plan provides this mapping for a specific product either explicitly or by reference to other documents. An understanding of the clinical context in which the product will be used will require appropriate clinical input.

E.3 Assignment of responsibilities and authorities

The clinical risk management plan should identify the personnel responsible for the execution of specific clinical risk management activities, for example reviewer(s), expert(s), independent verification specialist(s) and individual(s) with approval authority (see 4.2 and 4.3). This assignment can be included in a resource allocation matrix defined for the design project.

E.4 Requirements for review of clinical risk management activities

Review requirements are a responsibility of top management. The clinical risk management plan should detail how and when these management reviews will occur for a specific health software product. The requirements for the review of clinical risk management activities could be part of other quality system review requirements.

E.5 Criteria for clinical risk acceptability

Criteria for clinical risk acceptability are derived from the manufacturer's policy for determining acceptable clinical risk (see Annex H). The criteria can be common for similar categories of health software products.

Criteria for clinical risk acceptability can be part of the manufacturer’s established quality management system, which can be referenced in the clinical risk management plan.

E.6 Verification activities

Verifying the effectiveness of clinical risk control measures can require the collection of clinical data, usability studies, applicable test evidence, etc. The clinical risk management plan will specify how these distinct verification activities will be carried out. The clinical risk management plan can detail the verification activities explicitly or by reference to the plan for other verification activities.

E.7 Method(s) for obtaining relevant post-deployment information

The method(s) for obtaining post-deployment information can be part of established quality management system procedures. Manufacturers should establish generic procedures to collect information from various sources such as users, service personnel, training personnel, incident reports and customer feedback and should document how the information collected is to be used. While a reference to the quality management system procedures can suffice in most cases, product specific requirements should be directly added to the clinical risk management plan.

The clinical risk management plan should include documentation of decisions, based on a clinical risk analysis, about what sort of post deployment surveillance is appropriate for the product. For example, whether reactive surveillance is adequate or whether proactive studies are needed.

Annex F (informative) **Components of a generic risk management process**

F.1 Introduction

This annex provides a summary of what is required for successful risk management in general and thereby, for completeness, includes some aspects which are not in the scope of this standard, e.g. risks to those other than patients, such as to the business of system operators.

Normally the risk management process would be defined in quality management procedures and supported by life-cycle models and methods, as part of the clinical management system.

Successful application of risk management to health software involves a complex of independent processes which this Annex outlines.

At the highest level it requires:

- a complete understanding of the product/system;
- appropriate awareness of the need for risk management;
- the ability to identify relevant targets at risk;
- a fully defined risk assessment process;
- risk assessment to be carried out completely and competently;
- residual risks to be effectively presented/documented;
- appropriate life-cycle management to be in place.

Each of these in turn requires its own processes. These are outlined in the Clauses F.2 to F.8.

F.2 Achieving a complete understanding of the product/system

Achieving a complete understanding of the product/system requires:

- the product/system to be fully defined;
- the product/system's operation to be fully defined;
- the product/system's output to be fully defined;
- the product/system's operational environment to be fully understood;
- the product's operational dependencies to be fully understood;
- experienced and knowledgeable input.

F.3 Ensuring appropriate awareness of the need for risk management

Ensuring appropriate awareness of the need for risk management requires:

- awareness of risk management dictated by external requirements, such as:
    - risk management required by regulation,
    - risk management required through compliance with standards,

  - risk management needed to address other factors such as good corporate governance;
- awareness of risk management as part of project stages, such as:
  - risk management as part of design/development stage,
  - risk management as part of user/operational management.

F.4 Identification of relevant aspects at risk

Identification of relevant aspects at risk requires the ability to delineate:

- human risks, such as:
  - risks to those subject to the software, i.e. patients,
  - risks to operating personnel,
  - risks to third parties,
  - risks from patient interactions with software;
- whether risks are:
  - accidental,
  - deliberate;
- other risks, such as:
  - technical risks,
  - commercial/business risks,
  - environment risks,
  - security risks.

F.5 Ensuring a fully defined risk assessment process

Ensuring a fully defined risk assessment process requires:

- appropriate classifications/criteria to be in place, such as:
  - a hazard, risk and impact classification,
  - risk estimation criteria defined,
  - criteria for risk acceptability;
- appropriate assessment techniques to be defined/understood, including:
    - understanding hazard management techniques, such as:
    - hazard identification,
- risk analysis and evaluation;
  - understanding risk analysis techniques, such as:
    - hazard avoidance or mitigation,
    - risk evaluation.

F.6 Ensuring that risk assessment is carried out completely and competently

Ensuring risk assessment is carried out completely and competently requires:

- sufficient independence of the safety function;
- suitable effort to be applied to the process;
- sufficient effort to be applied to the process.

F.7 Ensuring that residual risks are effectively presented/documented

Ensuring that residual risks are effectively presented/documented requires:

- provision of details of the product/system;
- an explanation of the hazard and risk assessment process;
- an explanation of residual risks;
- an explanation of applicable constraints/dependencies;
- an explanation/justification of applied criteria;
- justification of applied competencies;
- identification of applicable management processes;
- identification and explanation of life-cycle issues.

F.8 Ensuring appropriate life-cycle management is in place

Ensuring appropriate life-cycle management is in place requires:

- use of risk management during concept and design phases;
- use of risk management during development production phases;
- use of risk management during implementation;
- effective management of residual risks during operational phases, including:
    - documentation of risks, constraints and dependencies,
    - putting in place operational risk management processes,
    - putting in place compliance assurance;
- consideration of appropriate decommissioning.

Annex G (informative) Relationship between clinical risk management file, clinical safety case, clinical safety case reports, stage reports and product life-cycle

G.1 The terms

The clinical risk management file is **the repository** of all records and other documents that are produced by the clinical risk management process. It is not a document but the place where all documents will be located or referenced. If referenced, the documents must be capable of being assembled in a timely fashion. The file may be in any form or type of medium.

The clinical safety case is **an argument, supported by a structured body of** evidence in the clinical risk management file that provides a compelling, comprehensible and valid case that a system is, as far as the clinical risk management process can reasonably ascertain, free from unacceptable clinical risk for its intended use. It evolves as the evidence and the argument mature through the life cycle of the product, e.g. from expert opinion and experience in use. It will usually be reviewed at particular points in the product lifecycle (see Clause G.2). For a complex system the argument and the supporting evidence may be a substantial set of documents.

A clinical safety case report is **a report that summarises** the arguments and evidence of the clinical safety case at a defined point in the health software's life cycle. It serves to communicate the clinical safety case, e.g. to customers or a regulatory authority. If the clinical safety case changes, e.g. due to experience in use, then a safety case report drawn from the clinical safety case will also need to change.

Stage reports are **the outcome of reviews** to allow progress to subsequent stages. The pre-release stage report is **the outcome of a particularly important review** undertaken before the product is released for distribution or deployment. The pre-release review is undertaken before distribution or deployment of the product to ensure that the clinical risk management plan has been appropriately implemented; the overall residual clinical risk is acceptable and that appropriate methods are in place to obtain post-deployment information. The report is aimed at those involved in the risk management process and top management to confirm that all that needed to be done has been done. It may be required also by others, e.g. a regulatory authority.

G.2 Relationship to product life-cycle

G.2.1 General

Figure G.1 demonstrates a possible life cycle for a software product and how a clinical safety case (CSC) will typically evolve through definitive stages. At defined points in the life cycle the clinical safety case may be reviewed. For each defined point in the life cycle there may be an associated clinical safety case report (CSCR).

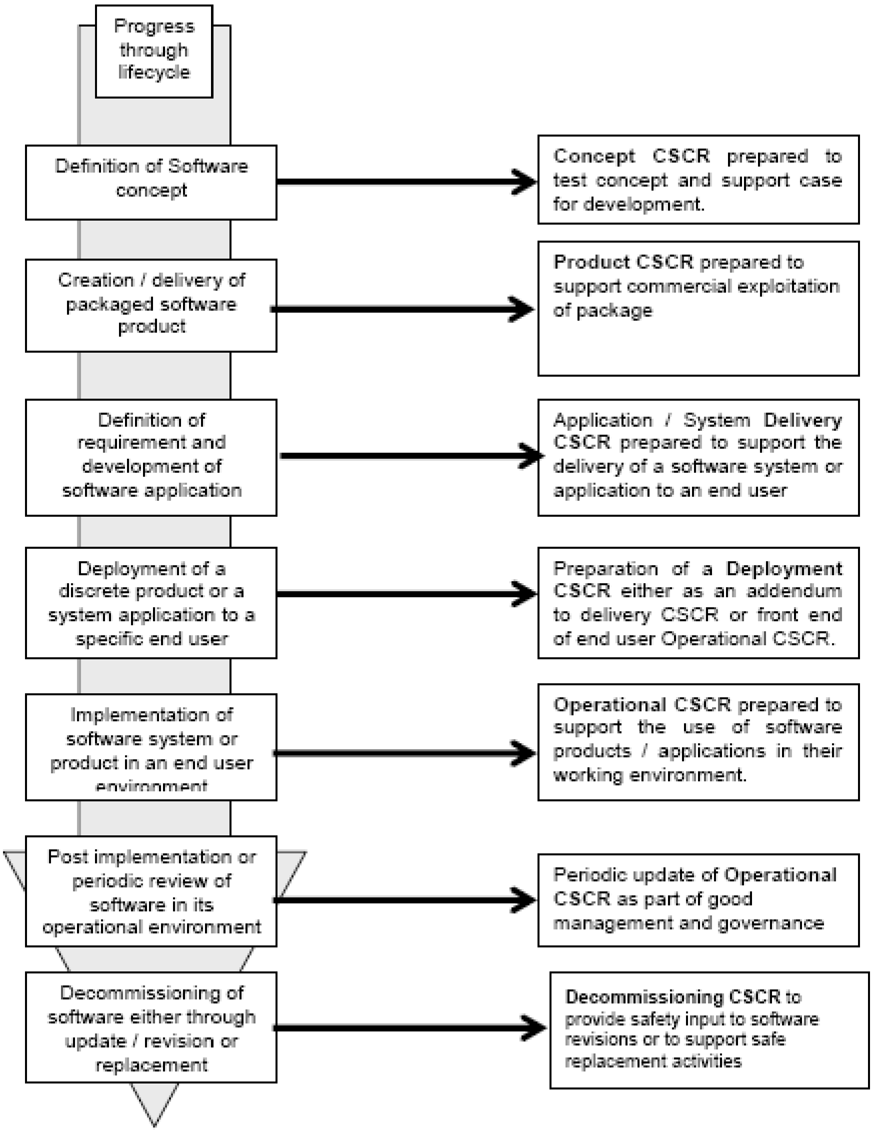
Progress through lifecycle
Definition of Software concept
Concept CSCR prepared to test concept and support case for development.
Creation / delivery of packaged software product
Product CSCR prepared to support commercial exploitation of package
Definition of requirement and development of software application
Application / System Delivery CSCR prepared to support the delivery of a software system or application to an end user
Deployment of a discrete product or a system application to a specific end user
Preparation of a Deployment CSCR either as an addendum to delivery CSCR or front end of end user Operational CSCR.
Implementation of software system or product in an end user environment
Operational CSCR prepared to support the use of software products / applications in their working environment.
Post implementation or periodic review of software in its operational environment
Periodic update of Operational CSCR as part of good management and governance
Decommissioning of software either through update / revision or replacement
Decommissioning CSCR to provide safety input to software revisions or to support safe replacement activities

Figure G.1 — Life-cycle stages and relevant clinical safety case reports

The life-cycle of a health software product extends from the initial concept evaluation, through design and development, into implementation and operation and finally to decommissioning. A clinical safety case report can be associated with each of these defined stages in this life-cycle and a review of the safety case may take place at each of these points.

A relevant set of life-cycle stages and related clinical safety case reports is shown in Figure G.1 and the different stages are described in G.2.2 to G.2.7.

In listing and describing a number of different clinical safety case reports which may arise at different points in the product life-cycle, it is recognised that some may be outside the manufacturer's responsibilities, e.g. the operational and decommissioning clinical safety case report. In many circumstances it will be the deployment clinical safety case report which will provide the interface between the manufacturer and the user. The operational and decommissioning clinical safety case reports will often be the responsibility of the user and thereby lie within the scope of ISO/TR 29322 [35]. Nevertheless the manufacturer will be capturing information from deployments of the software which will be feeding back in to the risk management process and therefore affecting the clinical safety case.

G.2.2 Concept clinical safety case report

This should be based upon the conceptual design of the health software product and its primary purpose would be to examine the possibility of developing a safe product to meet the conceptual requirements and to assess what clinical safety related controls would have to be put in place to make the concept feasible. The benefit of preparing a conceptual clinical safety case report is that the work carried out during its creation can be utilised during the detailed design phases, assuming the project is taken forward.

G.2.3 Product clinical safety case report

This is the point where the clinical safety case has reached the point of supporting a product ready for release but which may not necessarily relate to a specific operational environment but would contain information relating to its proposed use in defined clinical applications and environments. In particular it would contain details of any constraints or limitations in operation, which, if exceeded, could lead to a reduction in defined clinical safety levels.

G.2.4 Delivery clinical safety case report

This is similar to a product clinical safety case report but is intended to address circumstances where the manufacturer understands the intended working environment for the product or is working to the specific requirements of an end user. In this case the clinical safety case would include reference to a deployment hazard and risk assessment and wherever possible the hazard and risk registers and associated assessments would also relate to the operational environment.

G.2.5 Deployment clinical safety case report

In most situations the deployment of a specific health software product is closely related to its development process and in these cases the deployment clinical safety related issues would be addressed as part of a specific deployment review and then incorporated into the appropriate product or delivery clinical safety case report. However, it is feasible to deploy software products outside such arrangements and thus to develop a separate and dedicated clinical safety case report to cover such activity. It is particularly important to address issues relating to the transfer of functionality from an old system to a new product which may give rise to changes in apparent functionality and may require the migration of existing data. It should be noted that a completed deployment clinical safety case report is likely to contain information that can be of immediate benefit to the creation of a subsequent operational clinical safety case report.

G.2.6 Operational clinical safety case report

An operational clinical safety case report would address operational issues and build on a relevant product or delivery clinical safety case report. Its associated hazard and risk assessments would focus upon issues related to the day-to-day functionality and use of the product. The scope of the assessments would typically extend to encompass both normal and abnormal modes of operation and address emergency breakdowns and recovery procedures. An essential element of an operational clinical safety case report is most likely to be concerned with human factors and the possibility of operator or user error and the association of one manufacturer's product with others with which it is expected to interoperate.

An important principle of the generic safety case theory is that during the operational life of a software product or application, a number of safety critical factors may change. Amongst other things this could be due to personnel changes, working environment changes, changes effecting interfaces with other products or systems or simply the development of a better understanding of the original application. Thus it will be essential to periodically revisit the operational clinical safety case, to challenge its statements and to update it where necessary. It should be noted that this process may also bring about a need to alter operational procedures either to improve the operational process or to counter the incidence of bad operational practice.

G.2.7 Decommissioning clinical safety case report

All software products and applications have a limited life and at some stage will need to be decommissioned either in preparation for a revision or to be replaced. The clinical safety related issues arising out of this activity are very similar to those mentioned in relation to the deployment of a new product or application.

However, although it may be considered cost effective to address decommissioning only as part of the deployment of a new or replacement system, there are benefits in carrying out a decommissioning assessment in advance of an anticipated changeover in that such an assessment may raise issues that can be addressed before attempting to deploy the revised or replacement application. This is likely to improve the change-over experience and contribute to an overall reduction in residual risk. Decommissioning of a product may also significantly impact on the safe operation of other products with which it is interoperating.

Consideration of decommissioning hazards should also occur when deprecating or disabling individual functions or components during the life-cycle of the product and not be limited to the end of a product’s life.

Annex H (informative) **Clinical risk estimation and evaluation guidance**

H.1 General

This annex provides guidance on the following risk concepts important for managing the clinical risks of health software products:

- clinical risk analysis by means of classification,
- clinical risk acceptability,
- clinical risk control,
- clinical risk/benefit analysis, and
- overall clinical risk evaluation.

Clinical risk is defined in 2.2 as the combination of the likelihood of occurrence of harm to a patient and the severity of that harm.

This does not mean that the two factors are multiplied to arrive at a clinical risk value. One way to describe risk and to visualize the meaning of the definition is a two-dimensional risk matrix such as in Table H.1.

Table H.1 — General risk matrix

Likelihood	**Degree of severity**				
	Least				**Worst**
Highest					
Lowest					

Each cell of the matrix thereby represents a level of risk. Thus in the risk matrix above the 25 cells represent

25 risk outcomes which reduce in severity on moving diagonally from top right to bottom left.

H.2 Classification of likelihood of occurrence and degree of severity of harm to a patient

H.2.1 General

The following subclauses deal with classifying likelihood and severity and are given for illustrative purposes only. It is for the manufacturer to decide on the classification to use for a product. The illustrative classifications are drawn from CEN/TS 15260 [10]. There are other equally valid approaches and guidance such as that from the UK National Patient Safety Agency [31] or the approaches taken by such tools as CRAMM [17]. The risk evaluation criteria may be mandated by a standard or guideline in a particular country or region.

H.2.2 Likelihood of occurrence of harm to a patient

Health software products do not cause harm unless a sequence of events occurs to create a hazardous situation and that situation, within the clinical environment, then develops such that it actually causes harm. A hazardous situation occurs when a patient is exposed to a hazard. The hazardous situation may arise from a fault in the product but may arise even when there are no obvious faults, i.e. in the normal condition for the health software product. Furthermore, the likelihood of a fault is not the same as the likelihood of the occurrence of harm. A fault does not always result in a hazardous situation, and a hazardous situation does not always result in harm.

There are generally two types of faults that can lead to a hazardous situation, random and systematic faults.

Systematic faults are characteristic of software and, unlike random faults; the likelihood of their occurrence is not amenable to quantification. Thus their likelihood is subject to judgment on a qualitative scale and the likelihood of a hazardous situation arising will also be subject to judgement on a qualitative scale.

Note that a common definition of risk is 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”. This is for two reasons. As indicated above, the probability that a hazardous situation will arise 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 the safety of health informatics' products where such statistics and evidence are not available: 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 standard. Additionally this standard 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 definition refers to harm rather than other events in general.

The number of points on the qualitative scale is a matter of choice. The more the points the greater will be the ability to distinguish but the harder the assignment between adjacent points.

A five point scale might be:

- very high;
- high;

- medium;
- low;
- very low.

To these terms need to be attached a meaning to produce a possible classification as in Table H.2.

Table H.2 — Classification of likelihood of occurrence of harm

Likelihood of occurrence of harm	**Meaning**
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

H.2.3 Degree of severity of harm to a patient

As with “likelihood” the number of points on a qualitative scale for severity of harm is a matter of choice. A five point scale might be:

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

To these terms need to be attached a meaning to produce a possible classification as in Table H.3.

Table H.3 — Classification of degree of severity of harm

Consequence Category	Interpretation	
	Consequence	**Number of patients affected**
Catastrophic	Death	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.	Multiple

NOTE: This classification deals not only with physical injury but also with psychological trauma. The latter could, for example, arise from a security breach resulting in the revelation of a patient's HIV status. It also distinguishes between harm to single and to multiple patients.

H.3 Clinical risk acceptability matrix

The classifications in H.2.2 and H.2.3 can be used to create a clinical risk acceptability matrix as in Table H.4.

Table H.4 — Clinical risk acceptability matrix

Likelihood of occurrence of harm	**Degree of severity of harm to a patient**				
	Minor	Significant	Considerable	Major	Catastrophic
Very high	3	4	4	5	5
High	2	3	3	4 **(R1)**	5
Medium	2	2	3	3	4
Low	1	2	2	3 **(R2)**	4
Very low	1	1	2	2	3

To each cell can be assigned a clinical risk rating, e.g. to plan, prioritize and track clinical risk mitigation for example in a clinical risk register. Cells regarded as carrying clinical risks of a similar magnitude for the purposes of clinical risk management can be grouped. In Table H.4 cells have been grouped resulting in clinical risk categories 1 to 5 to which meaning could be assigned, e.g. unacceptable, acceptable. It is also possible to distinguish a clinical risk tolerance boundary (e.g. the broad line in Table H.4).

The following is an example of the application of these principles.

In the development of a prescribing system it is recognised that a hazardous situation could arise if a prescription was produced for a child but adult doses of a drug were prescribed. The possible degree of severity of the harm may be considered to be death, i.e. “major” and the likelihood of that degree of harm actually being realised may be regarded as “high”. This would result in a risk rating of 4 (R1 in Table H.4). To mitigate risk, the software is provided with a knowledge base to facilitate an alert to the prescriber if an adult dose is prescribed to a patient whose age indicates a child. This might reduce the likelihood of such instances to “low” albeit the severity of harm should the mitigation fail remains “major”. The risk rating thus drops to 3 (R2 in Table H.4). The risk nevertheless remains above the risk tolerance level. Since it may be impossible to guarantee that the system's knowledge base is 100 % accurate and always up to date in respect to child and adult dosages, it may be regarded as impossible to reduce likelihood further to “very low”. The manufacturer therefore informs the user of the residual clinical risk. The user may be able further to mitigate to “very low” through tightening administrative checks, e.g. in a hospital, in dispensing and, where applicable, administration.

Note this table and the example are for illustrative purposes only. It is for the manufacturer to decide on which rating to assign to each cell, on the positioning of any clinical risk within the matrix and on the positioning of any clinical risk tolerance boundary.

H.4 Acceptable clinical risk

This standard does not specify what is an acceptable clinical risk. That decision is for the manufacturer taking in to account, as far as practical, the current values of society perhaps expressed in local, national or regional regulations. Whatever the level chosen, it, and the rationale on which it is based, will need to be available to a user through the clinical safety case report (Clause 8 and Annex J). In this context the manufacturer will need to be aware of legal product liability.

H.5 Clinical risk/benefit analysis

Generally, if all practicable clinical risk control measures are insufficient to satisfy the clinical risk acceptability criteria in the clinical risk management plan, the design has to be abandoned. In some instances, however, greater clinical risks can sometimes be justified, if they are outweighed by the expected clinical benefits of using the product.

This Technical Specification allows manufacturers an opportunity to do a clinical risk/benefit analysis in exceptional circumstances to determine whether the clinical risk is acceptable based on clinical benefit.

The decision as to whether clinical risks are outweighed by benefits is essentially a matter of judgment by experienced and knowledgeable individuals which would normally include an appropriate and experienced clinician. Unfortunately, there is no standardized approach to estimate clinical benefit, and a greater degree of variation will be the inevitable result of using different approaches and of the greater subjectivity involved.

A clinical risk/benefit analysis is not required by this standard for every risk. A clinical risk/benefit analysis is used to justify a clinical risk once all practicable measures to reduce the clinical risk have been applied. If, after applying these measures, the clinical risk is still judged not acceptable, a clinical risk/benefit analysis is needed to establish whether the health software product is likely to provide more clinical benefit than harm.

Those involved in making clinical risk/benefit judgments have a responsibility to understand and take into account the technical, clinical, regulatory, economic, sociological and political context of their risk management decisions. This can involve an interpretation of fundamental requirements set out in applicable regulations or standards, as they apply to the product in question under the anticipated conditions of use.

If a clinical risk/benefit analysis leads to an acceptance of risks which otherwise fail the manufacturer's acceptability criteria, the decision, the circumstances and the rationale will need to be available to customers/users through the clinical safety case report (see Clause 8 and Annex J).

H.6 Overall residual risk evaluation

Overall residual risk evaluation is the point where the manufacturer has to step back and consider the combined impact of the individual residual risks on the use of the health software product.

The overall residual risk should be evaluated using the manufacturer's established risk acceptability criteria.

Overall residual risk evaluation needs to be performed by persons with the knowledge, experience, and authority to perform such tasks. It is often desirable to involve application specialists with knowledge of and experience with the health software product (see 4.3).

Overall residual risk evaluations can, however, become very complicated.

- A specific sequence of events can lead to several simultaneously occurring individual risks impacting together on the use of the product. Further analysis is often needed to identify any residual risks with a common cause. These risks need to be considered together.
- The resultant harm to a patient can originate from many hazards. Thus, to determine overall residual risk can require a top-down approach by, e.g., a fault tree-analysis to assess which sequence of events is most significant and needs to be controlled most effectively.

Since there is no standard method for evaluating overall residual risk, the manufacturer is responsible for determining an appropriate method.

H.7 “As low as reasonably practicable” (ALARP) approach

H.7.1 General

When establishing the risk acceptability policy, the manufacturer might find it convenient to use an “as low as reasonably **practicable**” (ALARP) approach to provide a practical basis for addressing the acceptability of the identified risks.

After a particular risk control option has been applied there are three possible results:

- the residual risk exceeds the manufacturer’s criterion for risk acceptability;
- the residual risk is acceptable because it is so small as to be insignificant; or
- the residual risk is between the two states above. For these risks the residual risk is acceptable for the option that reduces the risk to the lowest practicable level, bearing in mind the benefits resulting from its acceptance and taking into account the costs of any further reduction.

H.7.2 Residual risk is negligible

Below a chosen level the residual risk will be regarded as so insignificant that other options need not be investigated. This is the negligible region where the risks are comparable with the everyday risks we all normally tolerate.

H.7.3 Risk control option analysis

The as low as reasonably **practicable** approach can be used as part of risk control options analysis (see 7.2).

Risks for which the likelihood cannot be estimated would normally use the as low as reasonably practicable approach.

There is an important distinction to be made between residual risks that are so low that there is no need to consider them and residual risks which are greater than that but which are accepted because of the associated benefits and the impracticability of reducing the risks.

When a risk is estimated, the first question to be asked is whether the risk is already negligible and therefore there is no need to investigate risk reduction options. This decision is made once for each risk.

Risk reduction options are investigated for each risk that is not negligible. Risk reduction might or might not be practicable, but it should be considered. The possible outcomes are:

- one or more risk control measures brings the risk down to a negligible level and it is not necessary to consider it further; or
- whether or not some risk reduction is possible, reducing the risk down to a negligible level is not practicable.

Any specific residual risk that remains after the risk control measures are applied should be evaluated using the criteria defined in the risk management plan. If the residual risk does not exceed the manufacturer's criterion for risk acceptability and the as low as reasonably practicable approach has been applied, then no further risk reduction is necessary.

H.7.4 Practicability considerations

It might be thought that any risk associated with a health software product would be acceptable if the patient's health benefits. This cannot be used as a rationale for the acceptance of a practically avoidable risk.

All risks should be reduced to the lowest level practicable, bearing in mind the state of the art, the likely costs and the benefits of accepting the risk and the practicability of further reduction.

Practicability refers to the ability of a manufacturer to reduce risk. Practicability has two components:

- technical practicability; and
- economic practicability.

Technical practicability refers to the ability to reduce risk regardless of cost. The following are a few examples where technical practicability is questionable:

- including so many warning/caution labels that the user is hampered in operating the health software product;
- multiple alerts that create confusion;
- communicating so many residual risks that the operator has difficulty understanding which ones are really important or what to do;

- overly complex procedures for using the health software product so that the intended use is compromised; or
- using risk control measures that compromise the intended use.

Economic practicability refers to the ability to reduce risk without making the health software product an unsound economic proposition. These decisions necessarily involve making trade-offs between accepting risks and the availability of the benefits which the software product can bring. However, economic practicability should not be used as a rationale, or excuse, for the acceptance of practically avoidable risk.

Risks that clearly exceed the manufacturer’s criterion for risk acceptability should normally be reduced even if at considerable cost. Near the negligible region, further risk reduction will not be needed unless it can be easily accomplished.

H.8 “As low as reasonably achievable” approach

In some cases an “as low as reasonably **achievable**” approach is used. In this case the achievability, instead of the practicability, is taken into account. In effect this means only taking into account the technical practicability and ignoring the economic practicability.

Annex I (informative) Risk control guidance

I.1 Good design

The preferred approach to risk control is to reduce the exposure to risk through the application of good design which in this context could be defined as inherently safe design. Typically the root causes of hazards that lead to risks to patient safety arise either as a result of the specified functionality itself giving rise to a hazardous condition or through a fault or defect in the manufactured code. It is also possible that elaboration of specified functionality by the system engineers could generate outcomes with patient safety implications.

The preferred risk management option is that the initial hazard identification be carried out in parallel with the original requirements capture, elaboration and initial software design phases of the overall software development programme such that the developing product design can be updated and thus as many of these developing hazards as possible can be avoided. This would be a clear demonstration of good design but in recognition of practicability and commercial constraints it is unlikely to be possible to address all potential hazards. The overall hazard assessment process provides further means of risk reduction or mitigation and this therefore provides the complete risk management process.

I.2 Sufficiency and suitability of personnel and training

The rationale for a clinical safety case relies on the premise that the effectiveness of a delivered clinical safety case is based upon a demonstration that suitable and sufficient effort has been applied to conducting the hazard and risk assessment processes. There is no absolute measure of these attributes and therefore the premise requires that the manufacturer presents appropriate evidence within the clinical safety case and its associated report to illustrate that the processes and management constraints employed do meet acceptable standards. This can be justified either through specific compliance with relevant contractual controls or through a review of equivalent evidence in the public domain.

I.3 Structure and rigour of testing

In the same way that functional testing is typically seen as an essential contributor to the process of demonstrating that a product meets its specified requirements, the application of appropriate safety testing is seen as being essential to demonstrating the safety of health software. It should be recognised that safety implications can usually be identified both in respect of the functional requirements originally specified for the software as well as arising as a result of defects in the finalised product. The applied risk management process should have recorded the identified potential hazards in both these categories and documented ways in which these hazards should be reduced to acceptable levels of residual risk. The testing programme should address each of the initiating hazard scenarios and thus provide a practicable demonstration that the claimed risk reduction for each hazard has been achieved.

It is important to be able to confirm that all the relevant hazards have been addressed and this can be achieved by ensuring that the overall hazard assessment and risk reduction process incorporates suitable means to be able to trace the history of each residual risk, or avoided hazard, back to its initiating root cause.

The record of the test programme should also include details of the applied test procedures, including appropriate test scripts, in a way that justifies how the test has been used to examine each hazard scenario.

I.4 Adequacy of information at deployment

This standard provides for the preparation of a clinical safety cases' report at each stage in the overall health software product life-cycle as the clinical safety case evolves. There is also the requirement to conduct a review at each stage, the results of which are to be recorded in a stage report. These steps provide an input to subsequent stages. Where a single manufacturer is conducting a number of these stages it may be appropriate that less emphasis be given to the preparation of a comprehensive clinical safety case report as the delivery of information to the following stage since the manufacturer can rely heavily on the content of the risk management file. However, when a manufacturer reaches the stage where the health software is to be delivered or deployed to an end user, the clinical safety case report must be given increased significance. The target objective for this clinical safety case should be for it to contain sufficient information to provide the user with a complete picture of the safety of the health software and details of any operational constraints that should be maintained without the end user having to gain access to the risk management file.

I.5 Competency and training of personnel

The importance of patient safety demands that the conduct of hazard and risk assessments, the setting of tolerable criteria of acceptability, the approval of the resulting risk controls and the authority to accept the final level of residual risk associated with health software must be based upon the capability and judgements of suitably experienced persons. In this context, experience should reflect a wide variety of technical disciplines that contribute to the process.

It is of primary importance that recognition is given to the clinical aspects of the health software and that relevant clinical subject matter experts with appropriate clinical registrations are retained to conduct the clinical aspects of the assessments and clinical evaluations and are provided with the appropriate authority with regards to authorising the eventual deployment of the software. However, it is also important to recognise

that an effective safety assessment process requires the contribution of significant experience relating to the development of appropriate processes and management systems, the application and conduct of hazard and risk assessment techniques, the development of the software systems and the management of complex multidisciplinary teams.

This standard advocates the employment of multidisciplinary teams to compile the evolving health software clinical safety case and the justification of the clinical safety case needs to be based upon a demonstration of their competencies. It is therefore necessary to include a competency assessment and recording process alongside the clinical risk and safety process and this should be based upon a combination of experience and training.

I.6 Support and training of users

A critical aspect that influences the risks appertaining to the use of health software is the contribution to hazards that can be made by the operators and clinical users of the system. This is a factor that cannot be controlled directly by the manufacturer. However, it is a requirement that the manufacturer should identify to the user in the appropriate clinical safety case report the types of constraints that should be employed in the user environment to maintain the identified residual clinical risks within the given levels. This will probably give rise to a need for specific training of operators, particularly where operator actions or constraints on actions are being claimed as risk controls or mitigations.

It may therefore be necessary for a manufacturer of health software to include specific training within his overall clinical risk and safety management process. Details of any support, operator training and post deployment activities and procedures should be included in the relevant clinical safety case report.

Post deployment activities may also give rise to changes to the delivered version of the health software either as a complete revision or as the deployment of specific fixes or patches. This standard requires the application of the clinical risk management process to such changes and, within that context, any changes to, or additions to, training will need to be addressed.

I.7 Disclosure of information as a risk control measure

I.7.1 Introduction

The purpose of this clause is to provide guidance on how:

- information for clinical safety (see 7.2) can be implemented as a risk control measure;
- individual residual clinical risk(s) (see 7.4) can be disclosed; and
- the overall residual risk (see 7.8) can be disclosed in such a way as to control risks and promote risk awareness.

Risk control provided through information for clinical safety is accorded the lowest priority of risk control measures and is to be used in isolation only when other risk control measures have been exhausted.

Information for clinical safety gives instruction(s) on action(s) to take or not to take to avoid a risk. The information for clinical safety should be traceable to the risk analysis and should, wherever possible, be in addition to other risk control resources.

Disclosure of individual and overall residual risk(s) gives background and relevant information necessary to explain the residual risk so users can proactively take the appropriate and recommended actions to minimize exposure to the residual risk(s).

It should be recognized that both the structure and contents of the information as well as the implementation methods might need to be taken into consideration.

It should be recognized that information for clinical safety, in particular, might need to be implemented in different ways depending on when in the health software product life-cycle the information is to be communicated and to whom the information is intended, e.g. IT department or end user. An example is cautionary statements in the accompanying documents.

I.7.2 Information for clinical safety

When developing information for clinical safety it is important to identify to whom this information is to be provided and how it is to be implemented. The manufacturer should provide an explanation of the risk, the consequences of exposure and what should be done or avoided to prevent harm and to whom.

In developing the information, the manufacturer should consider:

- the level of priority appropriate to classify an action (danger, warning, caution, note, etc.);
- the location for the information for clinical safety (e.g. a warning label);
- the level or detail of information needed;
- the wording and/or pictures to be used to ensure clarity and understandability;
- the immediate recipients (e.g. users, service personnel, installers, patients);
- the appropriate media for providing the information, (e.g. instructions for use, labels, alerts); and
- regulatory requirements, etc.

I.7.3 Disclosure of individual and overall residual risk(s)

When developing the disclosure of individual or overall residual risk(s) it is important to identify what is to be communicated and to whom this is directed in order to inform, motivate and enable the user to use the product safely and effectively. The manufacturer should provide an explanation of the residual risk(s) identified in 7.4 and 7.8 to determine what should be disclosed.

The manufacturer should consider:

- the level of detail needed;
- the wording to be used to ensure clarity and understandability;
- the immediacy of the action sought;
- the immediate recipients (e.g. users, service personnel, installers, patients); and
- the means/media to be used.

I.7.4 Clinical safety case report

Notwithstanding other means for communicating to customers/users such as training manuals and user guides, the clinical safety case report will, in the context of clinical risk management, be an important means of communication to those responsible for health software safety in the user domain.

Annex J (informative) **Content of a clinical safety case report**

J.1 Background

Clause 8 lays down requirements for the content of a clinical safety case report as follows:

- Introduction and health software identification including:
  - general background;
  - unique identification details, including version;
  - detailed product description with details of intended operational environments and any critical constraints.
- Description of general and clinical safety management arrangements.
- Overview of hazard and risk assessment processes including risk evaluation and acceptance criteria covering:
  - identification of the conceptual hazard and risk methodology used;
  - justification of risk acceptance criteria;
  - justification of residual risk criteria.
- Identification and justification of any residual risks.
- Overall clinical safety justification.
- Lifetime management arrangements including:
  - performance monitoring arrangements;
  - incident/adverse event response arrangements;
  - lifetime support arrangements.

The following clauses provide further guidance.

J.2 Introduction and product description

The purpose of this section of the clinical safety case report is to provide descriptions of the product and its intended working environment and any constraints so as to provide a clear boundary within which the identified residual risks or customer implemented control measures apply.

This is important particularly where the software in question is one product that may be operated in a common environment with many other products, which may or may not have been developed by the manufacturer. This requirement is also very necessary to differentiate between different versions of the same product particularly where updates are developed to take account of subtle variations in an operating environment derived on a basis of operational experience or to take account of improvements to the software which may or may not address patches that have been applied in the course of time to the original product.

J.3 General and clinical safety management arrangements

Important factors that influence the safety of software relate to the reliability of the code that has been written to achieve the stated functionality of a product and the processes that are applied to manage the manufacturing activities and change management actions both during the development of the product and to deal with problems that arise post implementation as a result of live operations.

The general management of the manufacturing process should be compliant with a recognised management system approach and where this is achieved it should be sufficient to provide references to the relevant procedural documentation or system.

The management system for management of clinical safety in general should be outlined.

Particular reference to the management of change that takes place after the deployment of the software product or after the basic product safety case report has been prepared is important. The safety case report should demonstrate that such changes are properly assessed so as to ensure that they do not introduce any unacceptable additional risks to the utilisation of the software either directly as a result of a modification or by altering the basis of assessment of other parts of the software. The outcomes of such additions to the hazard and risk assessment processes and thus an updated clinical safety case should also be added to the product clinical safety case report either as a complete update or in the form of clearly identified appendices.

J.4 Overview of hazard identification and risk assessment process

The justification for the declared clinical safety of the software product is the application of suitable and sufficient hazard and risk assessment processes. The underlying requirement is to demonstrate rigour and practicability.

The generalized requirements for hazard and risk identification and assessment can be achieved through the application of any number of specific techniques and procedures and it is the responsibility of the competent risk and safety analyst to select an appropriate methodology for the product in hand.

This section of the clinical safety case report provides a description of the actual methodology employed including details of any applicable assumptions or constraints considered appropriate to the type of risks considered pertinent to the software under consideration.

Where appropriate, this section of the clinical safety case report should also include details as to how the hazard and risk assessment techniques and procedures are applied to any other activities associated with the software life-cycle that are directly associated with the manufacture of the product, such as deployment activities, adverse incident reporting and response and post implementation review and revision activities.

It is an acknowledged fact that it would be impossible to reduce the level of all associated risks to zero in any practicable situation. It is also reasonable to assume that a certain level of risk is tolerable in the user domain.

The derivation of appropriate classification and criteria of acceptability to be employed during the hazard and risk assessment processes is therefore a necessary and significant activity that should take account of both the probability or potential frequency of occurrence of the risk and the possible severity of the impact of the identified risks on patients. In some circumstances it may be possible for the manufacturer to reach a prior agreement with an end customer as to an appropriate basis for this criteria but alternatively it is necessary for a manufacturer to reveal in the clinical safety report the assessment made of the applicable level of risk tolerability based upon prevailing socio-economic or environmental factors. In either case, this section of the clinical safety case report needs to contain a detailed description of the applied classification and criteria together with supporting evidence justifying the decisions. This needs similarly to apply to justification of residual risk criteria.

J.5 Identification and justification of any residual risks

The clinical safety case report is intended to provide a user with a clear understanding of any residual risks that may arise from the application of the delivered software product. The important objective of this section of the clinical safety case report is to present a complete and coherent listing of such risks together with details of the constraints and limitations to operation upon which the stated level of residual risk is dependant.

This information is critical to the process of ensuring that the software is operated in a way that was taken into account by the manufacturer during the software design and development process and therefore forms the basis of acceptability of the software product in the actual user domain.

This section of the clinical safety case report does not need to include a presentation of all the content of the hazard and risk registers that have been compiled during the software development process and it should be sufficient to provide a reference to the appropriate clinical risk management file. However, this section of the safety case report needs to provide detailed information on all the contributing factors to the declared level of residual risk and needs to describe in detail the risk controls that must be introduced and maintained to keep the level of risk within the stated acceptable bounds.

J.6 Overall clinical safety justification

The individual sections of the clinical safety case report have been defined with the purpose of separately presenting specific aspects of the information that is considered necessary to deliver a statement concerning the clinical safety of a software product. This section of the clinical safety case report should be used to bring together the salient facts to provide a concise justification for the software product being delivered.

The principal argument shall demonstrate that suitable and sufficient effort has been applied to identifying and assessing all residual risks and that such risks are deemed acceptable on the basis of practicable and realistic criteria of acceptability.

An essential element of an effective clinical safety statement is the fact that both the software design and development and the hazard and risk assessment have been carried out by suitable qualified and experienced persons. Therefore, this section of the clinical safety case report should contain sufficient details to demonstrate the competencies of the personnel carrying out the relevant tasks and exercising authority to approve the findings of the completed clinical safety case report.

J.7 Lifetime management arrangements

This section should provide information on the manufacturer's arrangements for managing the product over its lifetime. It should include details of mechanisms the manufacturer has for post deployment monitoring which relies on customer feedback. The means which the manufacturer will utilise for providing customers with safety information and alerts should be described. This section should also, where appropriate, provide details of any ongoing support that the manufacturer is providing for the software, including help desks, product updates and other ongoing life-cycle arrangements.

Annex K (informative) Example structures of reports within a clinical risk management process

K.1 Introduction

The informative annex describes a selection of documents which might be found in a clinical risk management file as a result of risk and hazard assessment process tasks applied to the different stages of a typical software development process.

The example assumes that the manufacturer is responsible for the deployment of the software and demonstrates the process up to the preparation of a deployment clinical safety case complete with a deployment review. The whole is illustrated in Figure K.1. Other life-cycle clinical safety cases would entail a similar documentation structure using appropriate variations to the composition details provided in this example.

The extent of documentation etc. will depend on the complexity of the software product being developed. This example assumes a fairly complex product. The example also assumes that the client/customer is involved in specifying requirements: hence the reference from time to time to provision of information to the client/customer at early stages in development.

The process might typically be carried out by a clinical safety team working alongside software systems engineering development and production work streams employing an industry typical software development and production framework. The example implies a particular organizational structure involving personnel with particular titles/roles. This is for illustrative purposes only, i.e. it is not normative.

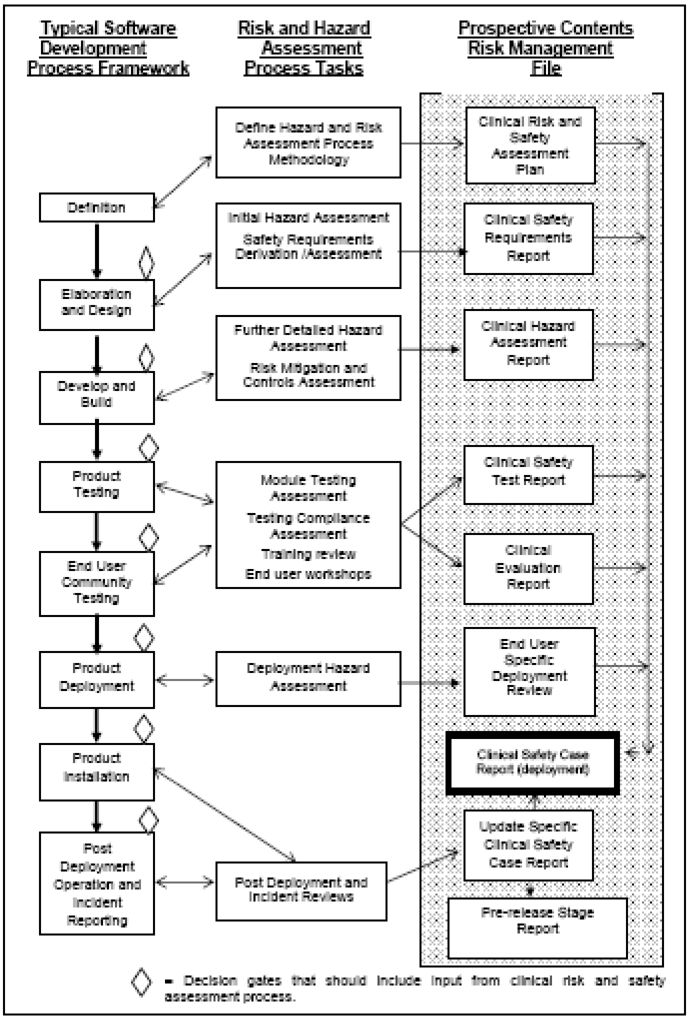
Typical Software Development Process Framework
Risk and Hazard Assessment Process Tasks
Prospective Contents Risk Management File
Definition
Elaboration and Design
Develop and Build
Product Testing
End User Community Testing
Product Deployment
Product Installation
Post Deployment Operation and Incident Reporting
Define Hazard and Risk Assessment Process Methodology
Initial Hazard Assessment
Safety Requirements Derivation /Assessment
Further Detailed Hazard Assessment
Risk Mitigation and Controls Assessment
Module Testing Assessment
Testing Compliance Assessment
Training review
End user workshops
Deployment Hazard Assessment
Post Deployment and Incident Reviews
Clinical Risk and Safety Assessment Plan
Clinical Safety Requirements Report
Clinical Hazard Assessment Report
Clinical Safety Test Report
Clinical Evaluation Report
End User Specific Deployment Review
Clinical Safety Case Report (deployment)
Update Specific Clinical Safety Case Report
Pre-release Stage Report
◇ = Decision gates that should include input from clinical risk and safety assessment process.

Figure K.1 — Document set in development process

K.2 Clinical risk and safety assessment plan

K.2.1 Purpose

The clinical risk and safety assessment plan is what other industries might call a safety process plan. The clinical risk and safety assessment plan sets out the safety-related activities, deliverables and milestones required from each workstream to compile a clinical safety case.

The clinical risk and safety assessment plan is here the primary method for communicating the above information to relevant project work streams. It also provides the criteria against which the stage reviews, including the pre-release stage review, are to be conducted and reports compiled.

K.2.2 Composition

The clinical risk and safety assessment plan documents the activities, deliverables and milestones from which a detailed 'Gant Chart' project plan can be created.

The clinical risk and safety assessment plan will include the following information:

- A summary of the safety-related scope for the release, derived from the release specification, of bundle maps or other available project documentation.
- A list of the artefacts to be produced to support the clinical safety case.
- An overview of the required activities and deliverables by workstream, including details of the safety representative from that workstream for the release.
- The activity based planning for each relevant workstream, that provides:
  - an overview of the impact on clinical safety of the workstream;
  - details of the clinical safety-related activities to be conducted by the workstream (in combination with, or overseen by, the clinical safety team);
  - deliverables required to be produced by the workstream (in combination with, or reviewed by, the clinical safety team);
  - milestones for each of the deliverables.
- The initial issue of the clinical risk and safety assessment plan may not normally contain complete details of the safety testing and clinical evaluation processes. These sections can be expanded in later issues of the clinical risk and safety assessment plan as more detailed information becomes available.

The plan will also address related management factors, namely pre-requisites and inputs, audience, attribution and quality and acceptance criteria as follows.

K.2.3 Pre-requisites and inputs

Pre-requisites:

- product or release functionality has been defined;
- timelines for each development gate are established/estimated.

Inputs:

- applicable safety management system;
- release specification;
- release development and production management plan.

K.2.4 Audience

The distribution list would typically include the directorate head for each of the following directorates:

- requirements
- development
- testing and integration
- deployment
- service management
- clinical safety team

In addition, this document would be sent to the following roles within the client's organization:

- clinical safety officer
- release manager

K.2.5 Attribution

Owner: head of clinical safety

Author: programme clinical safety manager, clinical safety team, with additional input from:

- product release manager
- appropriate healthcare specialist
- clinical safety team, systems safety engineer
- clinical safety team, safety test lead

K.2.6 Quality/acceptance criteria

For the clinical risk and safety assessment plan to be accepted it must:

- be consistent with the relevant corporate clinical safety management system;
- cover all work streams justifying where a workstream is not relevant for the release;
- include milestones of the activities and deliverables;
- indicate what is required for and what is required from each workstream.

Each Directorate should ensure that:

- the deliverables expected from them are consistent with their product descriptions;
- their plans include what is required from others and what they are required to deliver to others;
- any activities that they are to support are adequately resourced.

K.2.7 Quality skills/domain knowledge requirement

The following skills are required in the preparation of this product:

- a thorough understanding of the relevant corporate clinical safety management system;
- safety management knowledge to ensure that the activities specified will provide sufficient evidence that the clinical risks posed by the product/service have been reduced to acceptable levels;
- programme workstream knowledge to ensure that the required inputs and outputs from all contributors are relevant;

- project planning knowledge to ensure that the safety plan conforms to planning guidelines and is integrated into the release-level plan.

K.2.8 Review and approval procedure

The report should include details of the approval review and approval processes.

K.3 Clinical safety requirements' report

K.3.1 Purpose

The purpose of the clinical safety requirements report is to provide the means to communicate the safety related system requirements to all stakeholders, including:

- other work streams within the programme (particularly testing);
- suppliers of safety-related systems;
- the client.

There are two baselines for this report:

- the initial clinical safety requirements report is produced during the elaboration phase and identifies the safety-related system requirements;
- the full clinical safety requirements report is produced during the realisation phase. It provides an updated list of requirements and includes safety verification criteria for each of these derived requirements.

K.3.2 Composition

The clinical safety requirements report identifies safety requirements for a specified release. It provides systems engineering and the test centre with:

- safety requirements; (These are often derived requirements rather than customer requirements.)
- traceability from hazards to customer (or functional) requirements;
- safety verification criteria that can then be used as the basis for tests that demonstrate the effective control of identified hazards.

Where appropriate, the initial clinical safety requirements report will specifically include the following information:

- a summary of the safety-related scope of the product or release, derived from the release specification and taking into account all current contact change notices;
- details of all hazards associated with the service changes (that is, the functional aspects of the product or release) being introduced by the product or release;
- details of all hazards associated with any infrastructure changes (that is, the non-functional or architectural aspects of the product or release) being introduced by the product or release;
- details of all previously identified hazards that are still relevant for this product or release (for example, if a similar change is being introduced);

- a list of all functional and non-functional requirements that trace to one or more hazards.

The full clinical safety requirements report will in addition provide the following information:

- details of the verification criteria specific to the hazards, grouped by sub-system;
- a list of all safety-related training modules;
- a list of any dependencies on external systems, users or organizations.

At this point reference will be made to the hazard register where identified hazards and related information are being recorded. The following information will be provided for each hazard:

- the unique reference for the hazard (number);
- a concise title for the hazard (hazard);
- a precise description of the hazard at a system-level (hazard description);
- a description of the effect the occurrence of the hazard may have within the care setting and the impact on the patient (clinical impact);
- a description of how the hazard can be detected or the patient impact prevented within the care setting (clinical mitigation);
- potential causes of the hazard, grouped into system, human factors or external (causes);
- details of design features and system controls for the hazard grouped into system, human factors or external (controls);
- a risk assessment for the hazard (severity, likelihood and risk class).

The report will also address related management factors, namely pre-requisites and inputs, audience, attribution, and quality and acceptance criteria as outlined on the following subclauses.

An example of a hazard register is given in Table K.1

Table K.1 — Example hazard table

Hazard number	Hazard	Potential clinical impact	Possible causes	Mitigation and controls	Risk assessment
Unique number to identify each hazard	**Precise description of the system behaviour**	**Description of effect of hazard in care setting and potential impact on patient**	**Possible causes of the hazard (technical, human and external factors)**	**Internal and external**	**Categories for the severity and likelihood of hazard and risk class**
Example 1	Offline analysis used to reduce clinical risk not completed or completed incorrectly	Reports used to inform clinical decisions may be incorrect or misleading, which may result in the inability to intervene and address potential clinical risk	**Technical** Reports not configured to supply detailed information that may be required **Human** Information may have been entered incorrectly **External factors** Changes to mandatory datasets by other persons	**Internal** Certain screens contain mandatory fields ensuring collection of minimum dataset. Fields may be able to be changed through the change control procedure **External** Data held in other areas may be used to complete reports manually or through using other systems	**Minor x low = category 1**
Example 2	Background tasks including batch scheduled or deferred tasks not initiated or completed incorrectly	Errors in execution of batch scheduling, e.g. synchronization with other functions may not be detected and lead to inaccurate reports or a delay in patients receiving routine treatment. Clinical information may not be updated. The system may also delete appointments belonging to patients with an inappropriate death status	**Technical** Flaws in the detection or execution of batch processing **Human** Failure to review or understand the results of batch processing **External factors** Network outrage	**Internal** Functionality exists in system to allow validation that background processes have run correctly **External** Service management monitoring of system and communication facilities. Users should have network monitoring. Paper records may hold relevant information	**Significant x medium = category 2**
Example 3	Inadequate performance – particularly slow interactive performance or delays to transactions	Potential delays to treatment as information not available at the point of care. Information may not be recorded on paper and then not entered into the system resulting in missing clinical information within the system	**Technical** Failure of internal messaging modules. **Human** Users try to carry out to many commands at the same time. Users opening and utilising too many applications at same time **External factors** Denial of service attack on end user systems or communication facilities. Virus attack on end user clinical information systems	**Internal** Internal performance monitoring within system. Data centre security compliance procedures **External** Users trained before system use. Users should be using computers to supplier specifications. Users should have antivirus and network protection. Users can use paper etc. to add information provided by patient or others	**Significant x very low = category 1**

K.3.3 Pre-requisites and inputs

Pre-requisites:

- release content has been defined;
- a full assessment of the safety-related functionality for the product or release has been conducted.

Inputs:

- clinical risk and safety assessment plan;
- module use cases and non-functional requirements;
- contract change notices for the product or release;
- system architecture documents;
- hazard register for the product or release.

K.3.4 Audience

The clinical safety requirements report will be distributed to the product or release manager for each of the following programme work streams:

- requirements
- development
- deployment
- testing
- training

In addition, this document will be sent to the following roles within the client's organization:

- clinical safety officer
- release manager
- test manager

K.3.5 Attribution

Owner: head of clinical safety

Author: systems safety engineer

K.3.6 Quality/acceptance criteria

The following criteria must be demonstrated for the product to be accepted:

- the clinical safety requirements report must identify all functional and non-functional hazards that are relevant to the release (this does not include deployment hazards);

- the clinical safety requirements report must identify the safety-related functional and non-functional requirements for the product or release;
- the full clinical safety requirements report must specify verification criteria for each hazard and each safety related use case linked to the hazard;
- the full clinical safety requirements report must identify the safety-related training modules that will provide hazard mitigation.

K.3.7 Quality skills/domain knowledge requirement

The following skills are required in the preparation of this product:

- a thorough understanding of the relevant corporate clinical safety management system;
- safety engineering knowledge to ensure that the hazards are completely and correctly traced to the functionality specified for the product or release;
- requirements management knowledge to ensure that the hazards are traced to the correct requirements;
- clinical domain knowledge to ensure that the verification criteria provide an adequate basis to create clinical scenarios;
- testing knowledge to ensure that the verification criteria provide an adequate basis to create test specifications.

K.3.8 Review and approval procedure

The report should include details of the approval review and approval processes.

K.4 Clinical hazard assessment report

K.4.1 Purpose

The purpose of a clinical hazard assessment report is to provide a comprehensive listing of all the hazards' programme.

The preliminary clinical hazard assessment report contains an early snapshot of the hazard register and provides preliminary details on identified hazards. Since the preliminary clinical hazard assessment report is issued early in the life of a project, the hazard register will be necessarily incomplete in terms of identification of hazards, their mitigation and the assessment of residual risk. So, unlike the clinical hazard assessment report, the preliminary clinical hazard assessment report will not usually include information on likelihood and assessed risk but may include information on severity.

Identified for a specific product or release and a record of traceability that can be used to verify the outcomes of design changes and the resulting testing and clinical evaluation activities applied later in the development.

The full clinical hazard assessment report replaces the preliminary clinical hazard assessment report and is issued towards the end of the software development and production process.

The clinical hazard assessment report contains a snapshot of the hazard register and provides the customer with details on identified hazards, mitigation, controls and the residual risk for each hazard. This report will be issued towards the end of the development phase when the clinical safety case report is produced.

The contents of this report should be reviewed with customer representatives and potential users of the product to gain agreement on mitigation and residual risks.

The clinical hazard assessment report describes the safety features for product release, identifies the associated hazards and their impact in the clinical environment and assesses the level of clinical safety for the release, as determined from the hazard causes and controls.

The clinical hazard assessment report provides a definitive statement of the assessed hazards for product or release, draws conclusions about specific hazards (those with higher levels of assessed clinical safety risk) and the overall level of clinical safety risk, and makes recommendations for the mitigation of this risk.

The clinical hazard assessment report is produced in two baselines:

- the initial clinical hazard assessment report is produced during the definition phase and identifies the hazards and their impact;
- the full clinical hazard assessment report is produced during the design phase and is then completed at the end of the development phase and describes the mitigation features in the system design.

K.4.2 Composition

The hazard assessment will provide the following information:

- a summary of the functional and non-functional safety-related changes being introduced by the product or release;
- an overview of the assessment process that is followed and a list of the personnel involved in the assessment and their roles;
- an assessment of the clinical impact and any detection or mitigation mechanisms for each change;
- a summary of the deployment activities for the product or release (derived from the deployment plan) and an assessment of the related deployment hazards;
- a list of any assumptions on which the assessment is based;
- a discussion of the overall assessment results, summarising the number and type of hazards and the risk levels;
- a discussion of the intended mitigation approach for each hazard assessed with a significant, albeit tolerable, residual risk;
- a set of conclusions for the assessment and recommendations for risk reduction measures.

The report will also provide appendices containing the risk classification matrix, the hazard register extract and any relevant design information.

The report will also address related management factors, namely pre-requisites and inputs, audience, attribution and quality and acceptance criteria as follows.

K.4.3 Pre–requisites and inputs

Pre-requisites:

- product/release functionality has been defined;
- a full assessment of the safety-related functionality for the product or release has been conducted;
- a clinical hazard workshop has been conducted to review the results of the assessment;
- a full assessment of the method for deployment into live service has been conducted.

Inputs:

- clinical risk and safety assessment plan for the product or release;
- sub-system use cases and non-functional requirements;
- contract change notices for the product or release;
- sub-system system architecture documents;
- hazard register for the product or release.

K.4.4 Audience

The clinical hazard assessment report will be distributed to the product or release manager for each of the following programme work streams:

- requirements
- development
- deployment

In addition, this document will be sent to the following roles within the client's organization:

- clinical safety officer
- product or release manager

K.4.5 Attribution

Owner: head of clinical safety

Author: clinical risk lead

K.4.6 Quality/acceptance criteria

The following criteria must be demonstrated for the product to be accepted:

- the clinical hazard assessment report must identify all safety-related functionality for a product or release;
- the report must identify all hazards for the product or release;
- the report must specify the impact of each hazard and provide an assessed level of clinical safety risk;
- the report must provide an assessment of the overall level of clinical safety risk for the product or release;
- the full clinical hazard assessment report must identify a mitigation approach for each hazard assessed with a significant, albeit tolerable, residual risk;
- the full report must identify all relevant design features that provide mitigation for the identified hazards.

K.4.7 Quality skills/domain knowledge requirement

The following skills are required in the preparation of this product:

- safety engineering knowledge to ensure that the hazards are complete and correct according to the functionality specified for the product or release;
- clinical domain knowledge to identify the potential impact of system failures and any clinical mitigation in the clinical environment;
- system design knowledge to ensure that the description of the system safety-related features is correct.

K.4.8 Review and approval procedure

The report should include details of the approval review and approval processes.

K.5 Clinical safety test report

K.5.1 Purpose

The clinical safety test report presents the results of the module acceptance, system safety testing and clinical evaluation activities for the release or product and summarises and references supporting evidence that the system safety requirements have been implemented and verified.

The clinical safety test report provides evidence that the safety requirements have been implemented through the verification activities. There are four levels of verification:

- joint integration testing;
- module testing (functional and non-functional);
- clinical evaluation;
- client related integration testing.

K.5.2 Composition

The report will provide the following information:

- a summary of the hazards, including the system and human factor causes, and the associated verification criteria;
- the module acceptance report:
- a summary of the results of both producer and related client testing and the implications for system testing;
- a list of all the safety-related tests that have been applied;
- an evaluation of any outstanding safety-related defects.
- the system test report:
- a summary of the results of the system testing and the implications for system testing;
- a list of all the safety-related system functional and non-functional tests;
- an evaluation of any outstanding safety-related defects.
- a list of the safety-related tests to be run elsewhere and as model community testing.

The report will also address related management factors, namely pre-requisites and inputs, audience, attribution and quality and acceptance criteria as follows.

K.5.3 Pre-requisites and inputs

Pre-requisites:

- the full clinical safety requirements report has been issued.

Inputs:

- clinical safety requirements report;
- user interface documents;
- training scope document;
- training material;
- all the specific testing specifications and reports;
- system functional and non-functional test specifications and reports;
- any relevant integration and model community test lists.

K.5.4 Audience

The clinical safety test report will be distributed to the product or release manager for each of the following programme work streams:

- testing
- training
- clinical transformation team
- deployment team

In addition, this document will be sent to the following roles within the client's organization:

- test manager

K.5.5 Attribution

Owner: head of clinical safety

Author: safety test lead

K.5.6 Quality/acceptance criteria

The following criteria must be demonstrated for the product to be accepted:

- all levels of testing have been addressed within the report;
- the list of safety-related tests is traceable to the release safety requirements;
- the report provides an accurate summary of the results of the testing;
- all system causes of the hazards are covered by the test specifications;
- all human factor causes of the hazards are covered by the clinical scenarios;
- all outstanding safety-related defects have been addressed.

K.5.7 Quality skills/domain knowledge requirement

The following skills are required in the preparation of this product:

- safety engineering knowledge to ensure that the traceability between requirements and tests is correct;
- clinical domain knowledge to ensure that the clinical scenarios and the user interfaces reflect the required hazard mitigation;
- testing knowledge to ensure that the safety-related test evidence is adequate.
-

K.5.8 Review and approval procedure

The report should include details of the approval review and approval processes.

K.6 Clinical evaluation report

K.6.1 Purpose

The purpose of the clinical evaluation report is to provide evidence that demonstrates what has been done to assess the safety and clinical fitness for purpose of the system prior to deployment and final configuration.

K.6.2 Composition

This report will contain:

- Evidence concerning the clinical evaluation activities that were conducted and the result of these activities. For example:
  - a summary of the evaluation of all safety-related user interfaces;
  - a description of the safety-related training modules and a summary of the review of the training material;
  - the clinical test scenarios used with reference to the hazards that they cover;
  - a summary of the results of the clinical testing and recommendations for mitigation of identified issues.
- Evidence that all outstanding safety, clinical risk and usability issues have been risk assessed and that the residual risks have been reduced to a tolerable level.
- A list of any outstanding safety-related tests if applicable. For example, when evaluation of any clinical scenarios are planned to be run by the client.
- Recommendations, if any, for:
  - improvements to the product;
  - improvements to the clinical evaluation process;
  - tests that should be carried out following final configuration and prior to 'go-live'.

The report will also address related management factors, namely pre-requisites and inputs, audience, attribution and quality and acceptance criteria as follows.

K.6.3 Pre-requisites and inputs

Pre-requisites:

- the full clinical safety requirements report has been issued. (If required by the clinical risk and safety assessment plan.)

Inputs will vary depending on the content of the release but may include, for example:

- clinical safety requirements report;
- user interface documents;
- training scope document;
- training material;

- any relevant integration and model community test lists.

K.6.4 Audience

The clinical evaluation report will be distributed to the product or release manager for each of the following programme work streams:

- testing
- training
- clinical transformation team
- deployment team

K.6.5 Attribution

Owner: head of clinical safety

Author: health specialist assigned to lead the clinical evaluation

K.6.6 Quality/acceptance criteria

The following criteria must be demonstrated for the product to be accepted:

- all testing defined in the clinical evaluation section within the clinical risk and safety assessment plan has been addressed within the report;
- the report provides an accurate summary of the results of the testing;
- all human factor causes of the hazards are covered by the clinical scenarios;
- all outstanding safety-related issues raised during clinical evaluation are documented in the report.

K.6.7 Quality skills/domain knowledge requirement

The following skills are required in the preparation of this product:

- a thorough knowledge of the applicable safety management system and an understanding of how clinical evaluation supports the clinical safety case;
- clinical domain knowledge to ensure that the clinical scenarios and the user interfaces reflect the required hazard mitigation;
- testing knowledge to ensure that the safety-related test evidence obtained is adequate;
- knowledge and experience with the relevant product under evaluation;
- familiarity with the applicable testing software for documenting scenarios and acceptance criteria and recording results and “test issues”.

K.6.8 Review and approval procedure

The report should include details of the approval review and approval processes.

K.7 Clinical safety case report

K.7.1 Purpose and composition

The purpose and composition of the clinical safety case report has been described elsewhere in this Technical Specification (see Annex J).

K.7.2 Pre-requisites and inputs

Pre-requisites:

- all safety activities must be completed for the product or release.

Inputs, subject to modification in the clinical risk and safety assessment plan, include:

- clinical risk and safety assessment plan
- clinical hazard assessment report
- clinical safety requirements report
- clinical safety test report
- clinical evaluation report

K.7.3 Audience

The clinical safety case report will be distributed to the product or release manager for each of the following programme work streams:

- development manager
- deployment manager
- service manager

In addition, this document will be sent to the following roles within the client's organization:

- release manager
- clinical safety officer

The working environment specific deployment review will be provided to an approved representative from each of the end users for whom the product or release is being deployed.

The clinical safety case will be available to the customers(s) and any others with a legitimate need, e.g. regulators.

K.7.4 Attribution

Owner: director of clinical safety

Authors:

- release/product clinical safety case report: clinical risk lead
- trust-specific clinical safety case report: deployment safety lead

K.7.5 Quality/acceptance criteria

The following criteria must be demonstrated for the product to be accepted:

- all hazards identified by the hazard register are addressed within the report;
- all activities identified within the clinical risk and safety assessment plan are addressed within the report;
- the report is in compliance with Annex J of this Technical Specification.

K.7.6 Quality skills/domain knowledge requirement

The following skills are required in the preparation of this product:

- safety management knowledge to ensure that the conclusions drawn are correct and appropriate;
- clinical domain knowledge to ensure that relevant clinical information is included within the report;
- service management knowledge to ensure that information relevant to the operation of the product or release is included within the report.

K.7.7 Review and approval procedure

The report should include details of the approval review and approval processes.

K.8 Deployment review

K.8.1 Purpose

The purpose of the deployment review is to extend the scope of a delivery of a clinical safety case report to encompass aspects of the deployment process that are specific to the end user working environment.

K.8.2 Composition

The report will provide the following information:

- an executive summary stating the key points of the report;
- a summary description of the scope of supply and safety-related functionality for the specific release or version of the system that is to be deployed;
- a summary of the clinical safety and risk assessment activities undertaken that specifically relate to deployment issues relevant to the environment into which the system is to be deployed;
- a summary of the resulting hazard assessment results;
- a summary of all relevant information relating to:

- mitigation of the risk presented by individual hazards,
- appropriate rigour during the development activities,
- safe deployment of the system into the live environment,
- safe operation of the system by service management (where appropriate);
- reference should be made to the service incident management process (where appropriate);
- a summary of the results of any additional and specific safety reviews (for example, training, data migration, transition, etc.) conducted as part of the deployment process;
- a summary of any additional safety-related testing included within the deployment process;
- an evaluation of all hazards employing the same criteria as in the associated development process;
- a list of any outstanding issues or remaining activities to be conducted;
- assumptions and dependencies on other organizations to ensure that the level of risk remains acceptable while in service;
- an explanation of the criteria used for the risk management process;
- recommendations for further risk reduction measures to be communicated to the client and end user organizations.

The report will also address related management factors, namely pre-requisites and inputs, audience, attribution and quality and acceptance criteria as follows.

K.8.3 Pre-requisites and inputs

Pre-requisites:

- All safety activities must be completed for the product or release.

Inputs, subject to modification in the clinical risk and safety assessment plan, include:

- clinical risk and safety assessment plan;
- clinical hazard assessment report;
- clinical safety requirements report;
- clinical safety test report;
- clinical evaluation report;
- clinical safety case report (at least as a complete draft).

K.8.4 Audience

The deployment review will be attached to the relevant clinical safety case report and will be distributed to the product or release manager for each of the following programme work streams:

- development manager
- deployment manager
- service manager

In addition, these documents will be sent to the following roles within the client's organization:

- release manager
- clinical safety officer

The working environment specific deployment review will be provided to an approved representative from each of the end users for whom the product or release is being deployed.

K.8.5 Attribution

Owner: director of clinical safety

Author: deployment safety lead

K.8.6 Quality/acceptance criteria

The following criteria must be demonstrated for the product to be accepted:

- all hazards identified by the hazard register are addressed within the report;
- all activities identified within the clinical risk and safety assessment plan are addressed within the report.

K.8.7 Quality skills/domain knowledge requirement

The following skills are required in the preparation of this product:

- safety management knowledge to ensure that the conclusions drawn are correct and appropriate;
- clinical domain knowledge to ensure that relevant clinical information is included within the report;
- service management knowledge to ensure that information relevant to the operation of the product or release is included within the report.

K.8.8 Review and approval procedure

The report should include details of the approval review and approval processes.

K.9 Pre-release stage report

K.9.1 Purpose

The purpose of the pre-release stage report is to identify that all the risk management processes as detailed in the relevant clinical risk and safety assessment plan have been completed or to provide a detailed report on the status of the planned risk management processes with clear justifications regarding any outstanding or incomplete activities.

K.9.2 Composition

The report will contain the following information:

- an executive summary stating the key points of the report;
- a summary of the activities detailed in the final clinical risk and safety assessment plan;
- a confirmation of all the activities that have been completed making reference to the deliverable reports produced;
- details of any activities currently incomplete together with suitable explanations and anticipated outcomes;
- information regarding the location and access arrangements in place for future reference to or update of the risk management file.

The report will also address related management factors, namely pre-requisites and inputs, audience, attribution and quality and acceptance criteria as follows.

K.9.3 Pre-requisites and inputs

Pre-requisites:

- all safety activities have been completed for the product or release;
- the risk management file is be complete and up to date.

Inputs, subject to modification in the clinical risk and safety assessment plan, include:

- clinical risk and safety assessment plan;
- clinical hazard assessment report;
- clinical safety requirements report;
- clinical safety test report;
- clinical Evaluation Report;
- clinical safety case report (the draft pre-release stage report can be prepared in parallel with the clinical safety case report).

K.9.4 Audience

The pre-release stage report will be distributed to the product or release manager for each of the following programme work streams:

- development manager

- deployment manager
- service manager

In addition, this document will be sent to the following roles within the client's organization:

- release manager
- clinical safety officer

It will be sent to top management for final sign-off.

K.9.5 Attribution

Owner: director of clinical safety

Author: head of clinical safety

K.9.6 Quality/acceptance criteria

The following criteria must be demonstrated for the product to be accepted:

- the clinical safety case report is complete;
- all the tasks identified in the clinical risk and safety plan are completed or if not, suitable explanations can be provided;
- all activities identified within the clinical risk and safety assessment plan are addressed within the report.

K.9.7 Quality skills/domain knowledge requirement

The following skills are required in the preparation of this product:

- safety management knowledge to ensure that the conclusions drawn are correct and appropriate;
- clinical domain knowledge to ensure that relevant clinical information is included within the report;
- risk management file knowledge to ensure that information relevant to the status of the risk management process of the product or release is included within the report.

K.9.8 Review and approval procedure

The report should include details of the approval review and approval processes where the latter must include top management.

Bibliography

[1] OHN, 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 hospitalized 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] CEN/TS 15260:2006 and ISO/TS 25238:2007 Health informatics — Classification of safety risks from health software

[11] CEN/TR 15640:2007 and ISO/TR 27809:2007 Health informatics — Measures for ensuring patient safety of health software

[12] ISO/TMB Working Group on Risk Management. 1st Working Draft — Risk Management — Guidelines for Principles and Implementation of Risk Management, December 2005

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

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

[15] 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

[16] GHTF/SG3/NI5R8. Global Harmonization Task Force Study Group 3 — Risk Management Principles & Quality Management Systems, May 2005

[17] CRAMM. UK Government's preferred Risk Analysis & Management Method for Information Security Management, January 2003, www.CRAMM.com

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

[19] Measures for ensuring patient safety of health software (APSOHIP): Proposed next steps available from the CEN/TC 251 or TC 215 Secretariat

[20] ISO/DTR 80002, Medical device software – Guidance on the application of ISO 14971 to medical device software, CD 2008-05-06

[21] ISO/IEC 62304:2006, Medical device software — Software life cycle processes

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

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

[24] ISO 9001, Quality management systems — Requirements

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

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

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

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

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

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

[31] Risk Matrix Guidance for Patient Safety Risk Assessments, UK National Patient Safety Agency, March 2006 (www.npsa.nhs.uk)

[32] Def 00-56 “Safety Management Requirements for Defence Systems” Parts 1 and 2, UK Ministry of Defence, 2006

[33] Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

[34] WI IEC 80001, Application of risk management for IT-networks incorporating medical devices

[35] ISO/TR 29322:2008, Health informatics — Guidance on the management of clinical risk relating to the deployment and use of health software systems

[36] 2006 Annual Report of the Chief Medical Officer on the State of Public Health, Dirty hands – the human cost, Department of Health, www.dh.gov.uk/publications

[37] Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007 amending Council Directive 90/385/EEC on the approximation of the laws of the member states relating to active implantable medical devices, Council Directive 93/42/EEC concerning medical devices and Directive 98/8/EC concerning the placing of biocidal products on the market

[38] ASH, J.S., SITTIG, D.F., DYKSTRA, R.H. et al., Categorizing the unintended socio-technical consequences of computerized provider order entry. Int J Med Inf. 2007. 76(Supplement 1), p. 21-27

[39] BOBB, A.M., PAYNE, T.H. and GROSS, P.A., Viewpoint: Controversies Surrounding Use of Order Sets for Clinical Decision Support in Computerized Provider Order Entry. J Am Med Inform Assoc., 2007.14(1), p. 41-47