NHS Connecting for Health	**Health informatics - Guidance on the management of clinical risk relating to the deployment and use of health software (formerly ISO/TR 29322:2008(E)). DSCN18/2009**			
	Programme	NPFIT	**Document Record ID Key**	
	Sub-Prog / Project	Clinical Safety	NPFIT-FNT-TO-TOCLNSA-0831.01	
	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 — Guidance on the management of clinical risk relating to the deployment and use of health software
Formerly ISO/TR 29322:2008(E)
DSCN18/2009

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-0830.01	Health Informatics — Application of clinical risk management to the manufacture of health software (formerly ISO/TS 29321:2008(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 exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

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

ISO/TR 29322 was prepared by Technical Committee ISO/TC 215, Health informatics in collaboration with Technical Committee CEN/TC 251, Health informatics.

Note: NHS NHS CFH Clinical Safety Group, in agreement with the NHS Information Standards Board, have issued this paper as a cover document for TR29322 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/TR 29322:2008(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 TR29322. Any references to TS29322 in this document should be considered references to the document itself.

Introduction

The threat to patient safety

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

It is increasingly claimed that information systems such as decision support, protocols, guidelines and pathways could markedly reduce such adverse effects. If for no other reason – and there are others – this is leading to increasing deployment and use of increasingly complex health software systems, such as for decision support and disease management. It can also be anticipated that, due to pressures on time and to medico-legal aspects, clinicians will increasingly rely on such systems, with less questioning of their "output", as a "foreground" part of care delivery rather than as a "background" adjunct to it. Indeed, as such systems become integrated with medical care, any failure by clinicians to use standard support facilities may be criticised on legal grounds.

Increased use of such systems is not only in clinical treatment but also in areas just as important to patient safety, such as referral decision-making. Failure to make a "correct" referral, or to make one "in time", can have serious consequences.

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

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

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

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

Failures and deficiencies in health software systems can, of course, have adverse impacts other than causing harm to patients. They may, for example, create administrative inconvenience or even administrative chaos, with a range of impacts on the organization including financial loss. Harm to a patient may also have a consequent impact on the organization such as financial loss resulting from litigation.

Whereas these adverse organizational impacts will be significant, they are not the subject of this document unless they result in harm to a patient. It is the potential harm to the patient which is the subject of this document.

Controlling the risks

The safety of medicines and medical devices is ensured in many countries through a variety of legal and administrative measures which bear on manufacture. In the European Union, the safety of medical devices is subject to several EU directives, see references [7], [8], [9] and [36]. These measures are often backed by a range of safety related standards from a number of sources, both national and international, including the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and others. Some software, such as that necessary for the proper application or functioning of a medical device, is often encompassed by these legislative controls. Some software may be considered a medical device in its own right. However, there is software applied to health whose manufacture is not covered or is encompassed in a less than clear manner or is currently not a primary focus of some regulatory body. Thus there is health software whose safety in manufacture is not ensured by regulatory controls as a precursor to deployment and use.

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

A necessary pre-cursor for determining and implementing controls to minimize risks to patients, from a health software systems that is manufactured and then deployed and used within a health organization, is a clear understanding of the risks which the deployed system might present to patients if malfunction or an unintended event were to occur, and the likelihood of such a malfunction or event causing harm to the patient.

Additionally, if guidance is to be given to deployers and users of health software products then it will need to be recognised that the controls necessary for products presenting low risks are unlikely to be the same, or applied with the same rigour, as for those presenting high risks. The controls that are selected need to match both the level and types of risk that a product might present to a patient when deployed.

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

Conclusion 10 reads:

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

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

A companion Technical Specification ISO/TS 29321 [33] provides processes and other mechanisms for use by health software product manufacturers, whether these

be commercial entities or internal providers. Users of this Technical Report can, and should, place a greater degree of reliance upon commercial health software products that are manufactured and provided to them in accordance with ISO/TS 29321, then those that are not.

Relationship to Medical Devices

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

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

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

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

1 Scope

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

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

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

NOTE 2: Throughout this document the term “clinical” is used to make clear that the scope is limited to matters of risks to patient safety as distinct from other types of risk such as financial. The use of the term “clinical” should not be taken to mean that the persons involved in deployment and use are expected to be involved in clinical decisions affecting the treatment of patients in the direct clinical settings, unless this is consistent with some other aspect of their duties. This Technical Report however, makes clear that the assessment of risks to patients in the deployment and use of health software, and in decisions taken about those risks, needs to involve appropriate, experienced and knowledgeable clinicians.

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

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

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

2 Terms and definitions

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

2.1 Clinical hazard

Potential source of harm to a patient.

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

2.2 Clinical risk

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

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

2.3 Clinical risk analysis

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

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

2.4 Clinical risk assessment

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

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

2.5 Clinical risk control

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

2.6 Clinical risk estimation

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

2.7 Clinical risk evaluation

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

2.8 Clinical risk management

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

2.9 Clinical risk management file

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

2.10 Clinical safety

Freedom from unacceptable clinical risk to patients.

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

2.11 Clinical safety case

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

2.12 Clinical safety case report

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

2.13 Clinical safety management system

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

2.14 Harm

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

NOTE Adapted from ISO/IEC Guide 51:1999.

2.15 Hazardous situation

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

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

2.16 Health organization

Organization within which health software is deployed or used for a health purpose.

2.17 Health software product

Software product for use in the health sector for health related purposes.

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

2.18 Health software system

One or more software products from one or more manufacturers who operate together to support a health purpose.

2.19 Intended use

Use of a product, process or service in accordance with the specifications, instructions and information provided by the manufacturer to customers NOTE Information provided should contain references to the specific usages and environment to which the health software product, as part of a system, is intended to be put.

2.20 Life cycle

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

2.21 Manufacturer

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

2.22 Medical device

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

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

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

NOTE: This definition is drawn from the Global Harmonization Task Force (GHTF). Definition varies in detail from country to country.

2.23 Objective evidence

Data supporting the existence or verity of something.

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

[ISO 9000:2005, definition 3.8.1]

2.24 Patient

Any person who is the subject of a health-related activity which involves a software product.

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

2.25 Post-deployment

That part of the life cycle of the health software system after it has been manufactured, released, deployed and is ready for use by the health care organization.

2.26 Procedure

Specified way to carry out an activity or a process.

[ISO 9000:2000, definition 3.4.5]

2.27 Process

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

[ISO 9000:2000, definition 3.4.1]

2.28 Product

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

2.29 Record

Document stating results achieved or providing evidence of activities performed.

[ISO 9000:2000, definition 3.7.6]

2.30 Residual clinical risk

Clinical risk remaining after risk control measures have been taken.

NOTE ISO/IEC Guide 51:1999 [30], definition 3.9 uses the term “protective measures” rather than “risk control measures”. However, in the context of this Technical Report, “protective measures” are only one option for controlling risk as described in 6.2.

2.31 Responsible person

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

2.32 Severity

Measure of the significance of the possible consequences of a hazard

2.33 Top management

Person accountable directly to the chief executive or equivalent of a health organization.

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

2.34 Verification

Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

NOTE: Confirmation can comprise activities such as performing alternative calculations, comparing a new design specification with a similar proven design, undertaking tests and demonstrations, reviewing documents prior to issue and checking requirements have been addressed.

[ISO 9000:2000, definition 3.8.4]

3 Abbreviated terms

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

ALARP As Low As Reasonably Practicable

EU European Union

GHTF Global Harmonization Task Force

GP General practitioner

IT Information Technology

4 General approach

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

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

- Conclusion 8. If risk management is to be part of the requirements for ensuring the safety of health software products then a new standard, consistent at a high level with the results of ISO/TMB WG [12], ISO 14971 [13], ISO 61508-3 [14] and ISO 61508-5 [15], is required specifically for health software products. That standard should embody the concepts in GHTF/SG3/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.
- Conclusion 10. Standards for ensuring the safety of health software in the user environment should be addressed.

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

When addressing Conclusion 8 regarding clinical risk management in manufacture of health software, account needs to be taken of ISO 14971 [13]. ISO 14971 is widely used throughout the world for compliance with medical device manufacturing safety regulations. Such regulations for medical devices in most countries encompass software that is necessary for the proper application of a medical device or software that is an accessory to a medical device. In some jurisdictions, regulations also cover some other software and software may be considered a medical device in its own right. Thus medical device manufacturers are well experienced in the application of ISO 14971. Many manufacturers, particularly of electrical medical devices, are involved in the incorporation of software in medical devices, in producing software supporting such medical devices and/or producing software that is a medical device in its own right. A number of these manufacturers may also produce other health software of a type not encompassed by medical device regulations. Thus it would be advantageous to such manufacturers, regulators and those deploying and using such software, if the standard for the application of risk management to health software bore as close a relationship as practicable to ISO 14971. This was deemed practicable since, although ISO 14971 is devoted to medical devices, the essence of its requirements were equally applicable to health software.

Conclusion 8 has now been addressed in ISO/TS 29321 [33] and, for the reasons given above, that Technical Specification takes as its baseline ISO 14971. As far as practicable and appropriate the layout and requirements of the main text of ISO 14971 have been retained. Nevertheless one important additional requirement has been added, namely for the manufacturer of health software products to compile a clinical safety case and to make available to any customer a clinical safety case

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

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

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

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

4.2 Relationship with information security

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

In the construction of this Technical Report therefore, account has also been taken of ISO/IEC 27001 [18], that is founded upon risk management, and of ISO 20856 [34], that provides strong recommendations to health care organizations. In some jurisdictions, these International Standards may well have regulatory or legislative

support. Whatever may be the case, they will be of significant relevance to those seeking to deploy and to use health software systems.

4.3 Relationship with other elements of clinical and corporate governance

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

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

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

4.4 Life-cycle aspects

The life cycle of a health software system typically comprises:

a) concept development and requirements capture;

b) detailed design;

c) software development;

d) software verification;

e) software release/marketing;

f) system validation and deployment;

g) use;

h) decommissioning.

ISO/TS 29321 applies to all life-cycle stages in which the manufacturer is responsible; typically, these will typically be a) to c) although, depending on the contract, the customer may be involved in concept definition/design. This Technical Report applies to all those life-cycle stages for which the customer/health organization is responsible, which will normally at least include deployment, use and decommissioning, although an out-sourcing contract may place that in the hands of the manufacturer. However “deployment” can be in the hands of the manufacturer, the health organization or both. The manufacturer is likely, for example, to be heavily involved with the first deployment of a health software product as part of a health organization system. The standard which will apply to deployment will depend primarily on which body is responsible for ensuring patient safety. Where the manufacturer and the health organization work together on deployment and perhaps share responsibility for risk analysis etc., the manufacturer may work to ISO/TS 29321 (and thereby use the experience to build on the manufacturer clinical safety case) and the health organization may work to this Technical Report (using the experience to build the organization's clinical safety case and draw on the manufacturer's deployment clinical safety case report).

Since the hand-over from implementation in the user environment to live use will often involve the manufacturer/supplier and the user, a formal user acceptance protocol should be agreed upon and documented and include:

- a procedural work-through with users;
- and a dress rehearsal.

Whereas defining responsibilities for the purpose of determining which standard applies is important, the fact that the processes in ISO/TS 29321 and this Technical Report are the same makes the boundary less important.

4.5 The user environment

A health organization will typically have in place several, and perhaps many, health software products from a range of manufacturers, deployed as a range of systems. Many of these products may be interconnected and be expected to interoperate (perhaps on a network) as systems. They may be connected with health software systems in other health organizations. Even health software products that are not directly connected may have some sort of reliance on one another. When applying this Technical Report for the first time, some health organizations may already have in place a general risk management system (or a particular one, e.g. for security management) on which to build but others may have none. How to begin to implement this Technical Report for the first time may therefore be a significant problem in itself.

In starting from scratch the first challenge will be to carefully define the software system boundaries and the nature of the interfaces between the defined system (which may contain several software products) and systems outside the boundary. In this context it is important to note that the definition of a “health software system” in this Technical Report is “one or more software products from one or more manufacturers, which operate together to support a health purpose”. Thus the “system” which is to be the subject of the clinical risk management processes, and therefore the subject of this Technical Report, may encompass one or any number of software products and thereby encompass one or any number of applications new or existing or a combination of the two. In other words, the meaning and scope of the term “the system” in this Technical Report is that which is defined for the purpose of applying the risk management processes within this document. Compartmentalizing a complex system of interoperating products, such as in a hospital, is challenging and understanding the relationships and interfaces between components will be essential. It will be useful to remember that the compartmentalization is for the purpose of hazard and risk identification and the control/mitigation of those risks, and may therefore not coincide with other boundaries such as departments or specialities. As the risk management process is applied within each defined boundary within a system, it will be necessary to undertake iterative reviews to see whether one analysis impacts on another. Deciding where to start and what products and systems to address first may be assisted by crudely “classifying” products/systems according to the seriousness of the risks they may pose to patients such as described in EN TS 15260 [10].

In an ideal world the starting point for any risk analysis would be the clinical safety case reports from the manufacturers of each of the products involved within the defined system boundary i.e. the “output” from manufacturers applying ISO/TS

29321. However until that Technical Specification is widely applied such reports may not be available for products already in place. Customers should therefore require compliance with ISO/TS 29321 when buying new products. If clinical safety reports are not available from a manufacturer then the health organization's own clinical safety case will need to be built from scratch through the application of this Technical Report (whose processes are substantially the same as ISO/TS 29321).

As time progresses, health organizations will be involved in the simpler process of applying this Technical Report to the deployment of just one health software system, even if made up of a number of product components, which may be entirely new or the replacement or changing of an existing similar system. In that circumstance the deployment will be into a system which has already been the subject of risk management. The task will then be to apply this Technical Report in relation to the hazards/risks represented by the new/replacement product itself and the identification and control of any additional or changed risks which the new/replacement product may introduce into the system as a whole.

4.6 The basic processes

This Technical Report recommends that a health organization should:

- create a risk management plan which includes:
  - a careful delineation of the health software system to which the plan applies,
  - a staged approach defining the life-cycle elements to which the plan applies;
- assign sufficient resources to the plan's execution;
- create a clinical risk management file as the repository of all documentation;
- undertake a clinical hazard and risk evaluation;
- identify and implement risk control measures;
- identify residual risks;
- include in the risk management process an analysis of possible hazards and risks arising from software modifications, e.g. new versions, patches, changes;
- compile a clinical safety case for the defined health software system which:
  - will commence with the clinical safety case report(s) from the manufacturer(s) (if available),
  - will develop during the life cycle of the health software system,
  - will take in to account information gleaned from monitoring the use of the health software system;
- produce a clinical safety case report at defined points in the life cycle of the health software system to be provided particularly to users and to be created at least pre-use and pre-decommissioning, but also potentially when major changes are undertaken;
- implement a system for monitoring the health software system in use so as to identify any circumstance which may alter the risk assessment and to feed this back into the clinical safety case and, if appropriate, notify the manufacturer;
- review the whole risk management system regularly.

These matters should be conducted within the context of the organization's wider risk management policies and processes and any governance arrangements, e.g. for information/health informatics.

These matters are dealt with in detail in the following clauses.

4.7 Matching resources to system complexity and risk

Health organizations vary considerably in their organizational complexity and the complexity of installed IT. For example, a small GP practice and a large teaching hospital obviously present substantially different challenges for clinical risk management and consequently would require very different levels of resource and different administrative structures to undertake the risk management processes recommended in this Technical Report. Annex J considers this further.

5 General requirements for effective clinical risk management

5.1 Clinical risk management process

The responsible person should, for the health software for which she/he is responsible, establish, document and maintain, throughout the parts of the life cycle over which they have control, an ongoing process for identifying clinical hazards, estimating and evaluating the associated clinical risks, controlling these risks, and monitoring the effectiveness of the controls throughout the life cycle. This process, forming a clinical risk management system for health software, should include the following elements:

- identification of current situation, requirements, scope, extent of change to the current situation, impact and expected benefits;
- creation of a 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 and feedback to manufacturers;
- review and maintenance of clinical risk management process.

In complex environments the totality of an organization's installed software may be compartmentalized in order to be able to handle the complexity of risk analysis and other risk management processes. Defining the boundaries of each “compartment” and identifying and specifying the interfaces between “compartments” can be very challenging and it will be necessary to interrelate the clinical safety cases within each and identify any mutual interdependencies.

Annex D gives an example of the necessary components of a generic risk management process and lists of example entities to consider within that process.

5.2 Management responsibilities

Top management will need to provide evidence of its commitment to the clinical risk management process by ensuring the provision of sufficient resources and by the assignment of suitably qualified and experienced personnel (see 5.3) for clinical risk management.

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 in the organization. This function would normally address all aspects of operations and risk management that would bear upon clinical, i.e. patient and safety, aspects. Indeed, such a function would normally especially focus upon the degree to which such activity is consistent and integrated across the organization.

Top management should:

- define and document the organization's risk management policy including criteria for establishing clinical risk acceptability; this policy will need to ensure, where applicable, that criteria are based upon national, regional and/or sectoral or professional 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 to the deployment and use of the health software systems such that the risk management process can be efficiently and effectively applied, consistent with the complexity of the health software or system being deployed; at each stage, top management will need to sign off the appropriate stage report (see Clause 10);
- review the suitability of the clinical risk management process at planned, regular intervals to ensure the continuing effectiveness of the clinical risk management process and document any decisions and actions taken.

This review should be linked to the health care organization's clinical safety management system which in turn may be part of its quality management system or its enterprise risk management system, where these exist.

5.3 Competencies of personnel

Persons performing risk management tasks will need to have the knowledge, experience and competencies appropriate to the tasks assigned to them. This will need to include, where appropriate, knowledge and experience of the particular health software systems (or similar health software products) and applications, the technologies involved and risk management techniques. This should include appropriate registered clinical input throughout the process. Appropriate competency and experience records will need to be maintained.

Clinical risk management tasks can, and should, be performed by a project team that contains representatives of each of the functions that are involved in deploying and subsequently using the health software systems or system, with each contributing their specialist knowledge to build both awareness and consensus. Of particular

importance will be clinical input from clinicians who are familiar with the practical realities of the environments within which the software system will be used and the clinical processes to which the software system is directed.

5.4 Clinical risk management planning

Clinical risk management activities will need to be planned. Therefore, for the particular health software system being considered, the deploying organization will need to establish and document a clinical risk management plan in accordance with the clinical risk management process. The clinical risk management plan is part of the clinical risk management file.

This plan will need to include at least the following:

- the scope of the planned clinical risk management activities, including identifying and describing the health software system, what it is intended to do, how it will do it, the clinical context in which it will be used and the life-cycle phase(s) which the plan 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 and evaluation of the risks;
- criteria for assessing clinical risk acceptability, based on the organization's policy for determining acceptable clinical risk and which are fundamental to the overall success of the risk management process;
- verification activities;
- activities in case of changes to the health software system (e.g. patches, updates etc.);
- activities related to the collection and review of relevant post-deployment information and the feedback of that information both into the health organization's risk management processes and into the relevant manufacturers' processes, e.g. through health software systems, user groups or geographic communities or professional groups etc.

Annex C provides additional guidance on developing a clinical risk management plan. 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.

If the plan changes during the deployment, use or decommissioning stages of the health software product's life cycle, a record of the reasons for the change and the rationale for any changes in the relevant processes and application of those changes, will need to be maintained in the clinical risk management file.

5.5 Clinical risk management file

For the particular health software systems being considered for deployment and use, or for a given systems environment, the organization will need to establish and

maintain a clinical risk management file which is the repository of the documentation produced and which will need to provide suitable traceability. In addition to the requirements of other parts of this guidance, the clinical risk management file will need to provide traceability for each identified hazard to:

- the intended use, requirements and objectives of the health software system's deployment;
- the clinical safety case report(s) provided to the health organization by the health software products' manufacturer(s);
- the organization's subsequent further clinical risk analysis;
- the organization's subsequent further clinical risk evaluation;
- the organization's implementation and verification of the clinical risk control measures, including such clinical risk controls recommended by the manufacturer consistent with the health software system's intended use;
- the assessment of the acceptability of any residual clinical risk(s).

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 health organization's clinical safety management system, quality management system and/or enterprise risk management system. The clinical risk management file, as a virtual repository of all the relevant information and able to be in any form or type of medium, need not physically contain all the records and other documents relevant to risk management. However, effective best practice will require it to contain at least references or pointers to all required documentation and the associated version control references. The healthcare organization should be able to assemble the information referenced in the risk management file in a timely fashion.

Annex F provides more information on the relationship between the clinical risk management file, clinical safety case, clinical safety case report, pre-use stage report and clinical risk management review reports.

5.6 Clinical safety case

The organization deploying and using the manufactured health software system as part of a system's environment will need to develop and maintain a clinical safety case for the defined health software system. The clinical safety case argument together with its structured evidence needs to be identifiable within the risk management file.

The clinical safety case, as further defined in Annexes E and I, comprises an argument based on structured evidence demonstrating the clinical safety of the health software system, in the manner it has been deployed and then used. It will develop and evolve through the life-cycle stages of the software product(s) or system that are under the control of the deploying health organization, with the organization progressively building upon the system originally developed by the manufacturer(s) and provided to the organization by means of the clinical safety case report(s), that are further described in Annex I.

5.7 Intelligent procurement

Risks to patient safety can be considerably reduced through intelligent procurement. A formal framework for procurement should therefore be an integral component of risk management. Examples would be requirements in procurement contracts that the supplier/manufacturer:

- complies with ISO/TS 29321 and thereby makes available applicable safety case reports;
- complies with the organization's data and technical standards for interoperability, e.g. data definitions, codings and classifications, messaging conventions and structures, common screen display characteristics, external interfaces, etc. (these may in turn be based on national or international standards).

5.8 Non-health software products

Non-health software products can introduce a variety of risks particularly where health software is reliant upon them or interoperates with them. Risks may particularly arise with updates or patches applied to such products particularly when done in the background over, for example, the internet. Such non-health software products will not have been risk assessed for health applications and thus, where non-health and health software interact, the health organization will need to put in place its own appropriate risk management process.

Manufacturer's who comply with ISO/TS 29321 [33] are required to apply it to any health or non-health product which they incorporate into their health software and to reveal what they have done in this context in safety case reports. Customers should check what manufacturer's claim to have done and the extent of their contractual responsibilities for risk control both for original supply and for updates and patches which may be passed to the customer through them.

5.9 Customization, modification and updates

Many software products provide the facility for customization by the user. All the ways a customer might utilize such a facility may not have been considered as part of the manufacturer's hazard and risk analysis. Responsibility for the application of the risk management processes to local customization therefore falls to the customer. An essential starting point will be careful documentation of the customization undertaken. Assessment of consequential hazards and risks in collaboration with the manufacturer is advisable wherever practicable.

A useful tool for risk control will be a facility for user configured alerts and warnings although checks should be undertaken that these are well supported by evidence and local custom and do not introduce risks of their own.

Customers may undertake modifications to a product for local reasons in ways not facilitated or envisaged by the manufacturer and thus not encompassed by the manufacturer's own risk management processes. It needs to be recognised that such modifications can introduce risks which could be serious. Modifications should therefore be fully documented and included in the customer's risk management processes.

Manufacturers might declare to a customer that their product complies with a particular standard. Where such a standard is from an established standardization body, that can be advantageous. It should be noted however that some standards allow customization by manufacturers. Where this is so it will be for the manufacturer to apply appropriate risk management and to inform the customer appropriately.

Some health software might be supplied with so-called content software such as a coding and classification system, e.g. SNOMED. Such software will be regularly updated e.g. with new terms or codes. Whereas the manufacturer will have a responsibility to apply risk management to such updates, the customer will also have the responsibility for risk assessing the impact in use.

6 Clinical risk analysis

6.1 General

Clinical risk analysis is best conducted by a multi-disciplinary group including appropriate registered clinician(s). Organizations deploying and using health software products would also do well to obtain, either voluntarily or contractually, the involvement of their manufacturers [both of the new software product(s) and of any medical devices with which they inter-operate] in that group.

6.2 Clinical risk analysis process

Clinical risk analysis will need to be performed for particular health software systems in a structured and suitably comprehensive manner, as described in 6.3 to 6.5. Implementation of the planned clinical risk analysis activities and the results of the clinical risk analysis will need to be recorded in the clinical risk management file.

If a clinical risk analysis or other relevant information is available for a similar health software system, especially relating to its operational characteristics (i.e. when deployed and used), it can usefully be used as a starting point, provided that the differences are considered in order to identify 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 that the new product will introduce into the operational environment and the ways in which the differences can influence the development of various hazardous situations.

In addition to the records recommended in 6.3 to 6.5, the documentation of the conduct and results of the clinical risk analysis will need to include at least the following:

- a description and identification of the health software system that was analysed;
- identification of the person(s) who carried out the risk analysis;
- the scope and date of the clinical risk analysis, remembering that the health organization cannot readily afford to leave any product or system aspect out of its scope; the organization should therefore clearly document how it may have adjusted the depth of analysis to achieve a delivered result within its timescale and resource constraints.

The scope of clinical risk analysis can vary significantly and will need to be carefully considered and selected. It could be very broad and "shallow" (as in the earliest, conceptual stages of a new system with which the health organization may well have little or no experience) or "deep" (as the system's design matures and is developed) or the scope can be highly limited (e.g. when analysing the impact of a change to an existing product or system that is deployed and in use, for which analysis already exists in the relevant risk management file).

Some software may present particularly high potential risks and present considerable challenges. An example might be decision support software (see Annex H).

6.3 Intended use and identification of characteristics related to clinically safe deployment of the health software system

For the particular health software system being considered, the deploying organization will need to document the clinical scope and intended use and any reasonably foreseeable misuse, based on a clear understanding of the use environment. To enable this, the organization will need to identify the boundary of its review to avoid ending up effectively creating a clinical safety case for the whole organization. Whilst there is no single way of setting a boundary, it is likely to be best delivered at a "clinical process", "system" or "organizational function" level.

The organization will need to identify and document those qualitative and quantitative characteristics of the health software system that could affect the clinical safety of the (business and technical) environment into which it is deployed as well as its own intrinsic safety. A clear description of the ways in which the health software system's deployment will change the environment (with an especial focus on the technology changes and on any critical dependencies that will be introduced) will be fundamental to success.

In this context, misuse is intended to mean incorrect or improper installation, calibration, operation or use of the health software system. Since incorrect use may well depend on the human/computer interface, careful consideration of the "human factors" aspects should be included, for which specific expertise may need to be obtained.

Manufacturers of health software will typically provide release notes or similar with patches or updates of, or upgrades to, their health products. These will be a key source of input to the organization's deployment and use clinical risk management. If the manufacturer complies with ISO/TS 29321 [33] then a risk analysis associated with the patch or update will be available.

Health organizations will need to give an especial focus to the links/interfaces between products, as it would be unreasonable to expect manufacturers to have covered all possible linkages within their intended uses and thus their clinical risk management processes that culminated in the clinical safety case report(s) made available to the health organization.

These documents will need to be maintained in the clinical risk management file.

6.4 Identification of hazards to patients

The organization intending to deploy the health software system will need to compile documentation on known and foreseeable situations that represent hazards to

patients, in both normal and fault conditions. This documentation will need to consider such issues as:

- the key hazards, both with and without residual risks, as identified by the manufacturer(s) to the deploying organization, in its clinical safety case report(s), where these are provided;
- the operational requirements (e.g. knowledge base maintenance) and behaviour (e.g. processing power or communications link capacities) of the product(s) or system(s) components themselves;
- the pre-existing realities of the operational environment itself, into which the health software system is to be deployed;
- the practical interaction of users with the software and their behaviours once having used it;
- the interactions of the deployed health software system with other components, and the implications of those interactions for the operation (and thus safety) of those other components.

Even where the manufacturer(s) do provide clinical safety case reports, the health organization will need to consider the consequences and likelihoods of a failure of the manufacturers' controls to operate. The health organization will subsequently be in a position to identify:

- measures that it may require the manufacturer(s) to undertake either as part of its product development or contract for supply of the product(s) to that organization;
- the (additional) testing and validation that the health organization will undertake;
- the (complementary) controls that the health organization will implement.

This documentation will need to be maintained in the clinical risk management file.

6.5 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 will need to be considered and the resulting “realistic worst case hazardous situation scenario(s)” will need to be recorded.

For each identified situation that is hazardous to a patient, the risk(s) in both normal and fault conditions will need to 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 will need to be recorded in the clinical risk management file.

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

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

- manufacturers' clinical safety case report(s) as supplied to the organization;
- published standards;

- scientific technical data;
- field data from similar health software products and systems already in use, ideally in comparable environments, 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.

Annex G provides guidance on an approach to clinical risk estimation that could be employed by, or adapted for, the health organization.

7 Clinical risk evaluation

For each identified hazardous situation to a patient, the organization will need to decide, using the criteria it has defined in its clinical risk management plan, whether risk reduction is required for each individual risk. If risk reduction is not required, the requirements given in 8.2 to 8.6 do not apply for this particular risk (i.e. proceed to 8.7). The results of this clinical risk evaluation and the rationale on which it is based will need to be recorded in the clinical risk management file.

A key element of the clinical risk evaluation process should be to gain, as well as an understanding of the specific risk levels, an understanding of where the significant risks lie that may or may not subsequently be found capable of risk reduction to acceptable levels.

Guidance for deciding on risk acceptability is given in Annex F.

8 Clinical risk control

8.1 Clinical risk reduction

When clinical risk reduction is required, which it typically is in the delivery of health services, clinical risk control activities, as described in 8.2 to 8.7, will need to be performed.

Risk reduction can typically be achieved through a process of risk avoidance, risk control or risk mitigation. The preferred option is avoidance, i.e. where the originating hazard and its attendant risks are removed through alternative approaches to manufacture (if the health organization deploying and using the health software products can achieve that by working with the manufacturer during development or customization) or by deploying the resulting system in different ways/configurations.

Where it is not feasible to fully achieve this target, the next preferred process is to reduce the potential impact of a risk by implementing practicable changes to the operational environment in which the health software system will be deployed.

The least preferred method of clinical risk reduction is to develop controls or operational constraints, possibly through the medium of operator training and user warnings/advice, that, if properly employed, will result in the residual risk being maintained within the defined levels of risk that are considered tolerable or acceptable to the health organization. In this case, organizations deploying health software systems are likely to have received advice and guidance from the health software manufacturer(s), through their clinical safety case report(s), of controls that they would anticipate being implemented and especially of user training requirements. Health organizations either opting or obliged to take this route would therefore do well to obtain the manufacturers' engagement in such training whenever possible.

8.2 Clinical risk control option analysis

The deploying organization will need to identify clinical risk control measure(s) that are appropriate for reducing the clinical risk(s) to an acceptable level. Appropriateness of control measures will apply to the level and to the type of risk and also to the type of health software.

The health care organization will need to use one or more of the following clinical risk control options in the priority order listed:

- protective measures in the health software products themselves, or the system within which it is deployed, if this facilitates user customization/calibration to their particular environment;
- product verification and validation (e.g. testing);
- administrative and implementation procedures;
- user, operator and other stakeholder training and briefing;
- information for patient safety, including warnings.

The clinical risk control measures selected will need to be recorded in the clinical risk management file.

If, during clinical risk control option analysis, the health care organization determines that the clinical risk reduction required is not practicable, or other constraints mitigate against its implementation, then a clinical risk/benefit analysis of the residual clinical risk will be required (proceed to 8.5).

8.3 Implementation of clinical risk control measure(s)

The health care organization will need to implement the clinical risk control measure(s) selected in 8.2 in a structured and controlled manner.

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

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

8.4 Residual clinical risk evaluation

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

If the residual clinical risk is judged not acceptable using these criteria, further efforts will need to be invested, in either:

- additional clinical risk identification, estimation and evaluation at a more detailed level (see 8.1);
- additional clinical risk control measures (see 8.2 and 8.3).

For residual clinical risks that are judged acceptable, the health care organization will need to decide what information is necessary to include in the clinical safety case report(s) in order to suitably disclose the residual clinical risk to the user community and other relevant stakeholders, e.g. patients and staff.

The health organization should check whether national or regional regulatory requirements may apply and the health organization will also need to be aware of any other safety related legislation.

8.5 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 health care organization will need to 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 8.6.

For residual clinical risks that are judged acceptable, the health care organization will need to decide what information is necessary to include in the clinical safety case report(s) in order to suitably disclose the residual clinical risk to the user community and other relevant stakeholders, e.g. patients and staff.

The results of this evaluation will need to be recorded in the clinical risk management file.

8.6 Clinical risks arising from clinical risk control measures

The results of the clinical risk control measures will themselves need to be reviewed with regard to whether:

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

Any new or increased clinical risks will need to be managed in accordance with 8.4 to 8.5.

The results of this review will need to be recorded in the clinical risk management file.

8.7 Completeness of clinical risk control

The health care organization deploying and using health software will want to be able to demonstrate that the clinical risk(s) from all realistic hazardous situations to patients have been identified and considered and that a consensus has been achieved as to what the realistic worst case of their consequences and likelihood is obtained. The results of this activity will need to be recorded in the clinical risk management file.

8.8 Evaluation of overall residual clinical risk acceptability

After all clinical risk control measures have been implemented and verified, the organization will need to decide if the overall residual clinical risk posed by the health software system is acceptable. This is achieved 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 organization will need to re-review the data and literature previously collected 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 health organization will need to provide information that is sufficient to justify that assertion. Where an overall residual risk is judged unacceptable, and no further risk control options exist (i.e. 8.7 is confirmed), approval to deploy and use the system cannot be granted.

The results of the overall residual clinical risk evaluation will need to be recorded in the clinical risk management file.

9 Clinical safety case report(s)

The health care organization will need to compile a date-stamped clinical safety case report at each defined stage of the health software system development life-cycle for which they are responsible (i.e. normal deployment, use and de-commissioning).

The clinical safety case itself is an argument based on evolving experience and documentation (i.e. including that provided to health organizations by manufacturers) but will take definitive forms at “gateways” between the various stages of the product life-cycle.

Where, in complex environments, the organization's installed software is compartmentalized into a number of interoperating systems, the clinical safety case report for any one compartmentalized system will need to address any relationships and interdependencies with any other compartmentalized systems with which it interoperates or which it affects.

The reports therefore provide a vehicle for communication around clinical risks (particularly residual risks) to those with a legitimate interest or need. It will in particular provide the means of communication from the responsible person to end

users and top management. It may also be the means of communication for those from whom the organization will be keen to obtain positive engagement in system use, e.g. patients, voluntary bodies and perhaps the public at large. This wider communication may become increasingly necessary as patients and the public demand more understanding of the processes to which they are subjected.

Whenever any aspect of the clinical risk management process for the product or system is revisited, e.g. on the release by the manufacturer of an update or “patch” to their health software product that is a component of the health organization's health software system, or when the product as deployed within a system is interfaced with additional other applications, the results will need to be reflected in an updated clinical safety case report or “codicil” to the original report.

The clinical safety case report(s) or codicil(s) will need to be included in the clinical risk management file.

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

The health care organization will need to undertake a formal review, prior to release for live use, to ensure all that needs to be done, according to the risk management plan, has been done. The results of the review will need to be recorded in a stage report which will need to be signed off by top management of the health organization. This review will need to at least ensure that:

- the organization's clinical risk management plan has been appropriately implemented and the outcomes have been captured;
- the clinical safety case report(s) supplied by the health software product's manufacturer has been appropriately and comprehensively addressed;
- 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 and use information and to feed these back into both the organization's patient safety management system and into the manufacturer(s) of the system's product(s);
- a sufficient and accurate deployment and pre-use clinical safety report has been produced, in a form suitable for sharing with others.

The pre-use stage clinical safety report should not be confused with a clinical safety case report. The latter is a document specifically intended for communication, e.g. to the user, to demonstrate that the risks have been mitigated or reduced to acceptable levels. The pre-use 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 report(s) themselves] before the product or system is released into live use.

The allocation of responsibility for conduct of the pre-use clinical risk management review and for its sign-off should be assigned in the clinical risk management plan (see 5.4) and approved by the health organization's top management.

11 Post-deployment monitoring

Both manufacturers and organizations deploying and using health software and other products within systems, have a business need to establish, document and maintain a process to collect and review information about the clinical safety performance of the products and system in the post-deployment phase, at least to help manage their liabilities but also to enable them to optimize their products and systems.

When establishing a process to collect and review information about the health software system, the health organization will need to consider the mechanisms through which information generated by end-users or those accountable for the deployment, use and maintenance of the health software system, is collected and processed.

The information generated by such reporting will need to be evaluated to establish its relevance to the health software system's clinical safety, especially in the case of the following:

- if previously unrecognised hazards or hazardous situations to patients are found to be present when the product is deployed and used in practice;
- if the estimated clinical risk(s) arising from a hazardous situation to patients appears incorrect or is no longer acceptable to the health organization using the products within its systems' environment.

If the above conditions occur it will then be necessary for the health organization and manufacturer to collaborate to undertake, or at least share information to enable to be undertaken:

- a review of the clinical risk management file for the manufacture, deployment and use of the health software product and system; if there is a potential that the residual clinical risk(s) or its acceptability has changed, the impact on previously implemented and not implemented clinical risk control measures needs to be re-evaluated;
- the impact on, or effectiveness of, previously implemented clinical risk management activities, which will need to be fed back as an input to the clinical risk management process.

Manufacturers of health software products will typically 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. Health organizations will want to ensure that they have a process in place to both receive and assess this information in a suitably timely and rigorous manner.

Furthermore, manufacturers often establish “user groups” for products and health organizations will want to actively consider engagement in such groups to capture the benefits to them that “early warnings” and “peer experiences” will provide.

The health care organization deploying and using a health software system therefore has an essential role to play in post-deployment monitoring, in the best interests of all parties involved but not least in its own interests. Health organizations will therefore want to put in place appropriate arrangements for its own postuse monitoring both for its own purposes and as a source of input to the manufacturers' post-deployment monitoring arrangements.

This will especially be the case if some aspects of post-deployment monitoring are the subject of national or other regulations. In such cases, additional measures might then be required, e.g. electronic reporting of incidents.

The results of this evaluation will need to be recorded in the clinical risk management file.

12 Product modification

Health software systems that have been deployed and are in use are typically then subsequently quickly modified through release of amended versions, up-dates or “patches” and extensions of the functionality or use of the present functionality.

Whenever the product's deployment and use is modified, a suitable and sufficient clinical risk analysis, commensurate with the scale and extent of the modification (itself established by risk analysis), will need to be undertaken to establish what, if any, new clinical risks have been introduced.

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, e.g. an automatically released application “patch”, can potentially 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. However, it also needs to be performed expeditiously as the patch itself may well be intended to address a clinical safety risk. In effect, a miniature evaluation of overall residual clinical risk acceptability (see 8.8) may be needed as well as a similarly scaled clinical safety case report (see Clause 9).

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

13 Regular clinical risk management process review and maintenance

Health software products that have been deployed within systems are typically modified during their lifetimes but can also be replaced by successor systems, bringing their own life cycles to a close.

Health software systems that are being decommissioned from use will need to be subject to the same clinical risk management disciplines and processes as when they are first deployed and used. However, the process will now need also to be applied, in parallel, to the successor product's deployment and eventual use, if there is one.

The extent of the repeat clinical risk analysis will depend on the extent of differences to be found in the successor health software product(s) and will need to be considered from every perspective, such as:

- IT operational environment;
- product's functionality;
- product's information presentation approaches;

- user interaction approach.

Due rigour will need to be applied through the process, as there will be a range of critical considerations, such as ensuring:

- appropriate configuration of the new software product(s) within the system;
- conversion training of users;
- continuity of care;
- continuity of processing during the “cut over” period;
- continuity of data maintenance, management and transfer into the new system;
- appropriate archiving of data from the old system and any necessary transfers of data to the new system.

The decommissioning results will need to be recorded in the clinical risk management file and the clinical safety case amended as appropriate. Clearly, when there is a successor system, a new risk management file will need to be created and a new deployment clinical safety case commenced.

14 Compliance with this Technical Specification

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

The risk management process will need to be formally reviewed and reported regularly to top management, at least once a year. This will ensure that its place in any overall governance arrangements are kept under review and that experience and advancing techniques are taken on board. It is very easy to become complacent about processes when in truth they may need revitalising.

Such a review should encompass representatives of the key stakeholder communities and especially of the relevant clinical staff.

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.

In each case, the incidents could have been caused either during manufacture or subsequently in deployment, use or de-commissioning. This underscores the importance of overall health software clinical risk management and for strong co-operation across the two domains.

A.2 GP prescribing decision support

In 2004 the four most commonly used primary care systems 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.

The health organization clearly has, in such a system deployment, a key responsibility to ensure that knowledge bases used within a design are correctly populated and aligned with clinical practice within their organization.

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

This incident occurred when a user of a primary care 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 a 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.

This example again demonstrates the need to align clinical practice and authority levels with the knowledge and rule bases within the system. Wherever possible, design and implementation of health software systems should be undertaken to improve control and accuracy, note introduce new exposures. Furthermore the hazard and risk assessment of this situation may well not apply in other settings, e.g. prescription issue by nursing staff on a ward versus a pharmacist in a retail store.

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 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.

The manufacturer could have built in an appropriate format check during development. Alternatively, the problem could have been spotted by the health organization if a structured risk assessment had been undertaken.

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 need to establish a clinical data sharing policy, protocols and functionality in the new health software system. Because these were omitted from original commercial agreements and the subsequently developed products and system, the resulting delays gave rise to the potential for significant patient harm and operational difficulties that impacted the overall quality of patient care.

A.6 Drug mapping error

Sodium valproate 200 mg slow release was incorrectly mapped to sodium valproate 200 mg in a formulary encoded into a health software system. These are anti-epilepsy drugs and thus the implications for patient safety could be significant. This particular incident is just one of many that have been reported in relation 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 to check upon patient health and the supplier to correct the mapping process to ensure no further incorrect prescriptions were generated.

As before, this was a design/coding error by the manufacturer but was compounded by the health organization not checking the mappings and failing either to build in appropriate prescribing controls, or map the controls to health organization individuals with the appropriate experience and authority.

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 tests result 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 property. The health software system could have been designed to use unique numbers either instead of the name or in addition to it. User procedures for the system also lacked emphasis on checking the data entered.

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. Weaknesses in the design and or development of the health software system meant that calls coming in to the control room were not allocated to ambulances. Furthermore, because the system was being implemented in stages, an alarm which should have alerted staff to the problem was not working. This deficiency in deployment and use risk management 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, without the authority to do so. 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. The potential incident was averted only because a highly experienced nurse noted the extremely unusual combination of drugs, patient attributes and condition.

Investigation demonstrated that the hospital's software system was subject to poor security measures, including poorly mapped drug-to-patient mappings and a lack of staff training/awareness of secure system use.

Annex B (informative) **Conclusions of the CEN/ISO/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 level at some point in the future the controls will need to be founded on standards. The CEN/TR “Measures for ensuring patient safety of health software” [11] considered the standards needed and their nature. The conclusions are as follows.

a) If controls are to be proportionate to the risk which 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 15260:2006 [10] is deemed the most appropriate for such classification (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 that are significant for inter-working and inter-operability. 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], 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.

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) **Clinical risk management plan**

C.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 5.4.

The makeup and level of detail for the plan should be commensurate with the level of clinical risk associated with the health software system being deployed and used. The requirements identified in 5.4 are the minimum requirements for a clinical risk management plan. Health care organizations can include other items such as time-schedule, risk analysis tools, or a rationale for the choice of specific clinical risk acceptability criteria.

C.2 Risk management planning

All elements of the clinical risk management process should be mapped to the health organization's defined product deployment, use and decommissioning life-cycle stages. The applicability of those stages to this health software system should be captured in the clinical risk management plan, 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.

C.3 Assignment of responsibilities and authorities

The clinical risk management plan should identify the personnel with responsibility 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 5.3).

C.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 system's deployment or use. The requirements for the review of clinical risk management activities could be part of other quality system review requirements.

C.5 Criteria for clinical risk acceptability

Criteria for clinical risk acceptability are derived from the health organization's policy for determining acceptable clinical risk (see Annex F). The criteria can be common for similar categories of health software systems. Criteria for clinical risk acceptability can be part of the organization's established quality management, its clinical safety management system or its enterprise risk management system, which can be referenced in the clinical risk management plan.

C.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.

C.7 Method or methods for obtaining relevant information from actual use

The method or methods for obtaining health software system use information can be part of established quality management system procedures. Health organizations should establish generic procedures to collect information from various sources such as users, service personnel, training personnel, incident reports and other stakeholders' feedback and should document how the information collected is to be used. These procedures should also address how such information will be shared with the manufacturer(s) and with regulators etc. if this is required within particular jurisdictions.

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 surveillance is appropriate for the system when in use. For example, whether reactive surveillance is adequate or whether proactive studies are needed.

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

D.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 Technical Report, 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 safety management system.

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

At the highest level it requires:

- a complete understanding of the product/system to be deployed and used;
- appropriate awareness of the need for risk management;
- awareness of how risk management aligns with any wider governance processes;
- 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 D.2 to D.8.

D.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 and the impacts of such output on other products and/or devices;
- the product/system's operational environment to be fully understood;
- the product's operational dependencies to be fully understood;
- the product's impact on the technical operational environment to be fully understood;
- experienced and knowledgeable input.

D.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:
- regulations,
- obligations for compliance standard with,
- addressing other factors such as good corporate governance;
- awareness of risk management as part of project stage management, such as:
- risk management as part of development/deployment stages,
- risk management as part of use/operational management,
- risk management during change and decommissioning.

D.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 such as 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.

D.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,
- defined risk estimation criteria,
- criteria for risk acceptability;
- appropriate assessment techniques to be defined/understood, including:
- understanding techniques, such as:
- hazard identification,

- risk analysis and evaluation;
- understanding risk analysis techniques, such as:
- hazard avoidance or mitigation,
- risk evaluation.

D.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.

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

Ensuring that residual risks are effectively presented / documented requires the:

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

D.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 deployment and 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 E (informative) **Relationship between clinical risk management file, clinical safety case, clinical safety case reports, stage reports and product life-cycle**

E.1 Introduction

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, whether physical or logical, where all documents will be located or referenced. If referenced, the documents must be capable of being assembled in a timely fashion.

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 for deployment and use 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 through the life cycle of the product, e.g. from expert opinion and actual experience of the health software product(s) or system in use. It will usually be reviewed alongside each stage report (see Clause E.2). For a complex system, the argument and the supporting evidence may well be, and should be expected to be, a substantial set of documents.

A clinical safety case report is **a report that summarises** the arguments and key 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 particularly to the end users and top management but also where appropriate to others such as regulators and those to whom the health software system is intended to provide services. 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-use stage report is **the outcome of a particularly important review** undertaken by the health organization before the health software system is approved for live use or is decommissioned.

The pre-use review is undertaken to ensure that the clinical risk management plan agreed by the health organization has been appropriately implemented; that the overall residual clinical risk is acceptable and that appropriate methods are in place to obtain information from live use. 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. This stage report is therefore the output of a particularly important review, as it is effectively the point at which final “approval to operate” is given and is the last point when reasonably foreseeable risks can be prevented or mitigated in advance.

E.2 Relationship to product life-cycle

E.2.1 General

Figure E.1 demonstrates a possible life cycle for a health software system and how a clinical safety case (CSC) will typically evolve through definitive stages of manufacture and health organization deployment and use. At defined points in the life cycle, the clinical safety case may be reviewed. For each defined point in the life cycle there will typically be an associated clinical safety case report (CSCR).

Figure E.1 depicts a firm division of manufacturer and health organization roles, which may not always apply. In practice, the deployment CSC could fall into either entity's responsibilities, dependent on the contract specifications for the health software product's procurement.

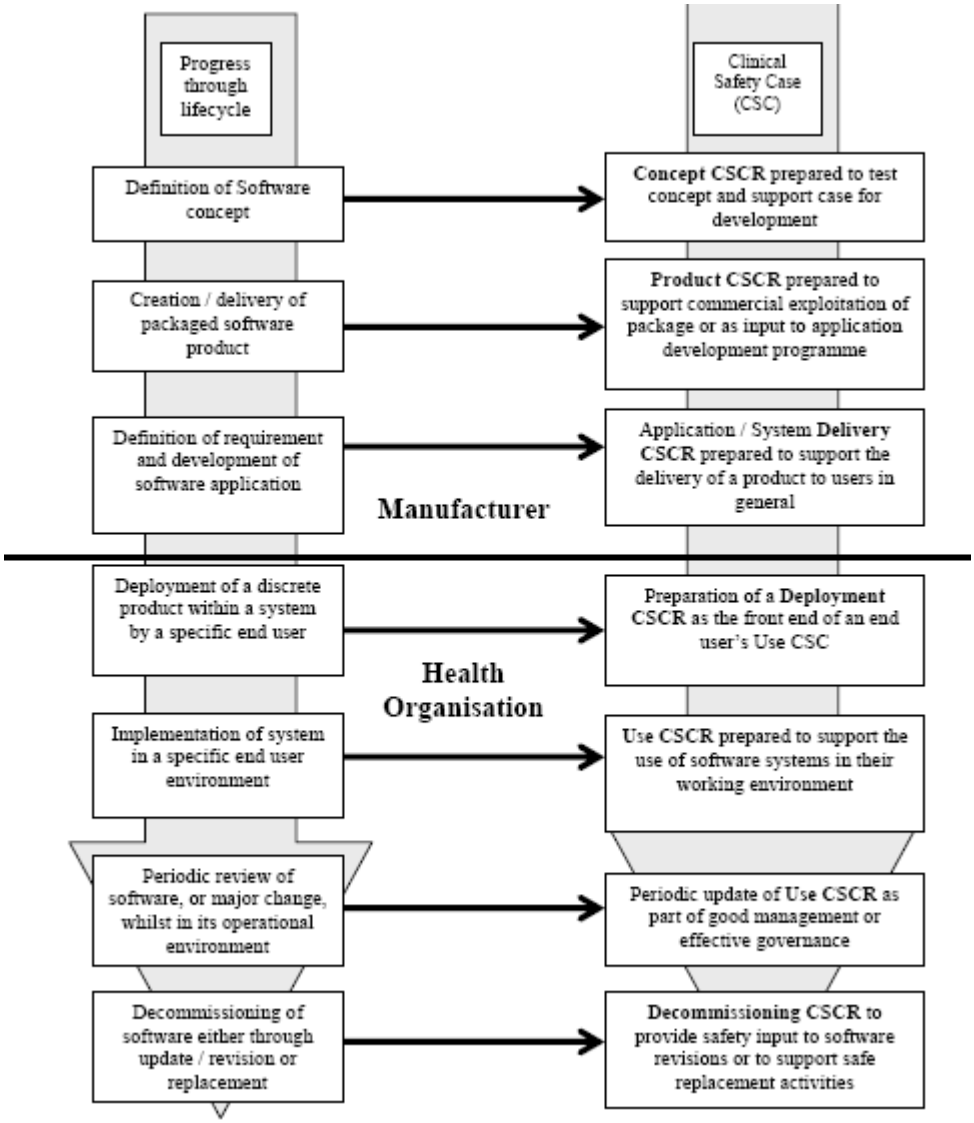

Figure E.1 — Life-cycle stages and relevant clinical safety case reports

A relevant set of life-cycle stages and related clinical safety case reports is shown in Figure E.1 and the different stages are described in E.2 to E.2.7. In listing and describing a number of different clinical safety case reports which arise at different points in the product life-cycle, some will be outside the deploying health

organization's control, e.g. the concept and development clinical safety case report, unless the health organization is also the manufacturer. In many circumstances it will be the delivery clinical safety case report that will provide the interface between the manufacturer and the health organization. However, health organizations seeking the development of unique health software may well need, typically by way of a development contract, to receive clinical safety case reports for the stages before deployment.

E.2.2 Concept clinical safety case report

This is based upon the conceptual design of the health software product(s) that together with other products or devices will make up systems for deployment and use. 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 utilized during the detailed design phases, assuming the project is taken forward, and also allows for significant hazardous situations and thus clinical risk avoidance.

E.2.3 Product clinical safety case report

This is created when 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. It would then 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.

E.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 report 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.

E.2.5 Deployment clinical safety case report

Although it is possible to deploy a software product almost “as delivered”, it is more likely that the processes of development and delivery are separate from its specific deployment and subsequent use. Thus a separate and dedicated clinical safety case report to cover deployment is then needed.

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 interaction of one manufacturer's product with others as part of the overall

system being deployed. To achieve these objectives, health organizations will need to have a very clear picture of the intended functions and use of the health software system in their specific situation.

E.2.6 Use clinical safety case report

A use clinical safety case report addresses the hazards related to day-to-day operation, maintenance and evolution of the health software system, including the clinical safety issues related to feedback received from end users. This clinical safety case report can only really be developed by the health organization which will be using the health software system that results.

An important principle of the underlying safety case theory is that during the operational life of a health software system, 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 and review the operational clinical safety case, to challenge its statements and to update it, and of course the controls environment that been implemented, where necessary.

E.2.7 Decommissioning clinical safety case report

All software products and systems 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 are very similar to those mentioned in relation to deployment. 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 F (informative) Clinical risk estimation and evaluation guidance

F.1 General

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

- clinical risk analysis by means of classification,
- clinical risk acceptability,
- clinical risk control,
- clinical risk/benefit analysis,
- 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 F.1.

Table F.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, some of which will be the same, but which reduce in severity on moving diagonally from top right to bottom left.

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

F.2.1 General

Subclauses F.2.2 and F.2.3 deal with classifying likelihood and severity and are given for illustrative purposes only. It is for the health organization to decide on the classifications to use for a deployed product or system, although consistency between different employments of the process will be important.

The illustrative classifications are drawn from EN TS 15260 [10]. There are other equally valid approaches and guidance such as that from the UK National Patient Safety Agency “Risk Matrix Patient Safety Risk Assessments” [31] and the approaches taken by such tools as CRAMM [17] which already recognise patient safety implications from security breaches – including in relation to software.

F.2.2 Likelihood of occurrence of harm to a patient

Health software systems 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 systems, e.g. in misuse or unanticipated abnormal conditions not envisaged by the manufacturer or health organization's intended uses. 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 fault that can lead to a hazardous situation, random faults 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, typically best arrived at by way of a consensus, 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 Report 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 as yet available, such that qualitative judgements are then necessary. Whereas probability can of course be qualitatively expressed, the term “likelihood” better conveys that meaning and is therefore used in this Technical Report. Additionally, this document 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 allow consistency of application and to produce a possible classification as in Table F.2.

Table F.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

The above process will need to be applied to the full range of potential/applicable hazards. The following are examples that should be considered and whose selection should be on the basis of their relevance to the clinical safety of the system being evaluated:

- masquerading of user identity by insiders;
- masquerading of user identity by contracted service providers;
- masquerading of user identity by outsiders;
- unauthorized use of an application;
- introduction of damaging or disruptive software;
- misuse of system resources;
- communications infiltration;
- communications interception;
- communications manipulation;
- repudiation;
- communications failure;
- embedding of malicious code;
- accidental mis-routing;
- technical failure of host;
- technical failure of storage facility;
- technical failure of print facility;
- technical failure of network distribution component;
- technical failure of network gateway;
- technical failure of network management or operation host;

- technical failure of network interface;
- technical failure of network service;
- power failure;
- air conditioning failure;
- system and network software failure;
- application software failure;
- operations error;
- hardware maintenance error;
- software maintenance error;
- user error;
- system administrator error;
- knowledge management error;
- rule base error;
- fire;
- water damage;
- natural disaster;
- staff shortage;
- theft by insiders;
- theft by outsiders;
- wilful damage by insiders;
- wilful damage by outsiders;
- terrorism.

This list will need to be amended to suit the attributes of the health software system being evaluated in the context of its intended use(s).

F.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 allow consistency of application and to produce a possible classification as in Table F.3.

Table F.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

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 unintended disclosure of a patient's HIV status. It also distinguishes between harm to single and to multiple patients.

The assessment of the degree of severity of harm to a patient will also need to be considered in terms of a variety of different impact types. An example list would be as

follows, although most will apply to any health software system being considered in respect of its clinical safety:

- physical destruction;
- system unavailability for different time periods, e.g. 15 min or less, to more than a month;
- data destruction, either total or since the last successful back-up;
- disclosure to insiders, service providers and to outsiders;
- modification whether small scale, wide-spread or deliberate;
- systems interference including insertion, non-delivery, replay, out-of-sequence, misrouting and repudiation.

F.3 Clinical risk acceptability matrix

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

Table F.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 F.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 F.4).

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

In the deployment and use of a prescribing system in a health organization 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, e.g. because of errors in a rule base used to assess proposed dosages or simple mis-use by the clinician using the system. 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 realized may be regarded as “high”. This would result in a risk rating of 4 (R1 in the Table F.4).

To mitigate risk, the manufacturer will hopefully have ensured clinical involvement, and especially approval, of the rule base and access controls to that rule base in a “change mode”. If it is possible to over-ride the rule base, the software could provide a knowledge base to facilitate an alert to the prescriber (or their manager) if an adult dose is prescribed to a patient whose age indicates a child. This might reduce the likelihood of such instances to “low” although the severity of harm, should the mitigation fail, remains “major”. The risk rating thus drops to 3 (R2 in Table F.4) and might be considered acceptable/reasonable by the manufacturer, especially if they were to also warn the deploying health organization and recommend specific training of users. The health organization might still not consider the risk level acceptable and could decide to utilize the access control features to limit prescribing to a limited set of users.

The risk might then be considered to fall below the risk tolerance level (R3 on Table F.4) set by the health organization, making deployment and use acceptable. Note that this table and the example are for illustrative purposes only. It is for the health organization 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 its clinical risk tolerance boundary.

F.4 Acceptable clinical risk

This Technical Report does not specify what is an acceptable clinical risk. That decision is for the health organization, taking into 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 health organization's clinical safety case report (see Clause 9).

F.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 proposed deployment and use shall be abandoned as “unsafe”. 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 Report assumes that the health organization may wish to carry out 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 can be 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 recommended by this Technical Report 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 system 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 organization's acceptability criteria, the decision, the circumstances and the rationale will need to be available to interested parties and especially users through the clinical safety case report (see Clause 9).

F.6 Overall residual risk evaluation

Overall residual risk evaluation is the point where the organization deploying and using a health software system has to take a step back and consider the combined impact of the individual residual risks on the use of the health software.

The overall residual risk should be evaluated using the organization'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(s) or system (see 5.3).

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 risks 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 health care organization remains responsible for determining an appropriate method.

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

F.7.1 General

When establishing the risk acceptability policy, the health organization 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 agreed criterion for risk acceptability;
- the residual risk is acceptable because it is so small as to be insignificant;

- 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 (intolerable) costs involved in any further reduction.

F.7.2 Residual risk is negligible

Below a pre-selected level, the residual risk will be regarded as sufficiently small as to be tolerable. As such, no other options need be investigated. This is the negligible region where the risks are comparable with the everyday risks we all normally tolerate.

F.7.3 Risk control option analysis

The as low as reasonably **practicable** approach can be used as part of risk control options analysis (see 8.2). 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 that 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 already 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;
- 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 health organization's criterion for risk acceptability and the as low as reasonably practicable approach has been applied, then no further risk reduction is necessary.

F.7.4 Practicability considerations

It might be thought that any risk associated with a health software system 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 involved and the benefits of accepting the risk and the practicability of further reduction.

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

- technical practicability;
- 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 systems or system;
- 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 system so that the intended use is compromised;
- using risk control measures that compromise the intended use.

Economic practicability refers to the ability to reduce risk without making the deployment and use of the health software system an unsound economic proposition.

These decisions necessarily involve making trade-offs between accepting risks and the availability of the benefits which the software can bring. However, economic practicability should not be used as a rationale, or excuse, for the acceptance of a practically avoidable risk.

Risks that clearly exceed the organization'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. On the other hand, if such risk reduction has a high economic cost then the clinical safety case and or “business case” for deploying has to be considered as unmade and the proposed deployment and use to be unsafe.

F.8 “As low as reasonably achievable” approach

In some cases therefore, 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. This is increasingly the case in health care but also an acceptable practice in that it is empirically demonstrable, in as much as it is in practice the process typically applied in actual health services delivery.

Annex G (informative) Risk control guidance

G.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 both to the original manufacture of the health software product(s) and to the manner in which they are deployed and used as systems.

The preferred risk management option is that the initial hazard identification be carried out in parallel with the original requirements capture, elaboration and "deployment design" phases for the software to allow the maximum opportunities for deployment hazard avoidance.

G.2 Sufficiency and suitability of personnel and training

The rationale for a clinical safety case relies on the premise that the rigour, comprehensiveness and 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 recommends that the health organization 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.

G.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 during manufacture, the subsequent application of appropriate safety testing is essential to demonstrate that the inherent safety of the health software products has not been subverted by the way in which the health organization deploys and uses the subsequent system.

It should be recognised that safety implications can usually be identified in respect of the functional requirements originally specified for the software but also from defects in the finalised product and from the manner in which it is deployed and used. 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, a major element of which will be testing.

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. The record of the test programme should also include details of the applied test procedures, including appropriate test scripts, in a way that both justifies and allows trace back of how the test has been used to verify the mitigation of each hazard scenario.

G.4 Competency and training of user personnel

It is of primary importance that recognition be given to the clinical operation aspects of the health software system and that relevant training, ideally led by clinical and technical subject matter experts, be undertaken.

Such training should focus upon the contribution to both the creation of hazards, and conversely their mitigation, that can be made by the operators and users of the health software system. This is a factor that, whilst it cannot be controlled directly by the manufacturer, is directly addressable by the health organization deploying and using the health software system. It is however, reasonable for a health organization to expect the manufacturer to identify to the health organization, through the use of warnings and other such messages, the types of constraints that should be employed in the user environment to maintain the identified residual clinical risks within the proposed 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 helpful for a health organization to contract specifically with the manufacturer(s) of health software products to include specific training within the services they deliver.

Changes to the version of the health software product(s) deployed and used, in the form of a complete revision, the implementation of specific fixes or patches, or the further enhancement of the product(s) or system will all give rise to new risks and, by definition, to new training needs. Suitable and sufficient training should be seen as a mandatory component of the health organization's change in management process.

G.5 Disclosure of information as a risk control measure

G.5.1 Introduction

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

- information for clinical safety (see 8.2) can itself be implemented as a risk control measure;
- individual residual risk(s) (see 8.4) can be disclosed;
- the overall residual risk (see 8.8) can be disclosed in such a way as to control risks and promote risk awareness.

Risk control provided through the provision of information for clinical safety is accorded the lowest priority as a risk control measure and is to be used in isolation only when no other risk control measures have been identified. 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, whenever 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 recognised 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 recognised that information for clinical safety, in particular, might need to be implemented in different ways depending on when in the health software system's life cycle the information is to be communicated and to whom the information is intended, e.g. for an IT department or end user. An example is cautionary statements or warnings in the accompanying documents.

G.5.2 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 health organization 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 health organization should consider:

- the level of priority appropriate to the information (danger, warning, caution, note, etc.) and the potential use of graphics to attract attention: this is analogous to what is found on instructions for use for consumer products;
- 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 immediacy of the action sought;
- the appropriate media for providing the information, (e.g. instructions for use, labels, alerts, training materials;
- regulatory requirements.

G.6 Controls suitable for the operational environment

The following list provides a generally well recognised list of types of controls that are suitable for ensuring the patient safety of the operational and/or overall environment. However, not all these types of control will be applicable in every instance.

Table G.1 — Types of control

Table G.1 — Types of control	
Identification and authentication	**User identifiers**
	Password length
	Password storage
	Password generation
	Password use
	Identification of a user by token or biometric devices
	Frequency of password change
	Password distribution
	Log-on dialogue
	Duress alarm
	Workstation identification
	User authentication for external connections
Logical access control	Discretionary access control
	Data labelling
	Mandatory access control
	Workstation time-out
	Limitation of connection time
	Data encryption (storage)
	Accountability for assets
	User registration
	Privilege management
	Review user access rights
	Access control policy
	Restrictions on access to information
	Sensitive system isolation
	Security of application system files
	Protection of audit trails
	Security of electronic office systems
Accounting	Event logging
Accounting *(Continued)*	Clock synchronization

Table G.1 — Types of control	
Identification and authentication	**User identifiers**
	Trusted facilities management
	Retention of accounting log
	Accounting log capacity
Audit	Auditing tools
	Review event log
	Investigation of incidents
	System audit controls
	Protection of system audit tools
Object re-use	Secure deletion procedures
	Secure deletion
Security testing	System security acceptance criteria
	Conduct of security testing
Software integrity	Software integrity checks
Protection against malicious software	Prevention against malicious software
	Detection of malicious software
	Removal of malicious software
Mobile computing and teleworking	Mobile computing
	Teleworking
	Security of equipment off-premises
Software change controls	Software change authorization
	Change auditing
	Emergency fixes to software
Software distribution	Receiving software
	Exporting software
System input/output controls	Input/output device identification
	Exporting data
	Exporting data and its classification/protective marking
Network security management	Information and software exchange agreements
Network security management *(Continued)*	Network management
	Network monitoring

Table G.1 — Types of control	
Identification and authentication	**User identifiers**
	Security of network services
	Evasion of network disruption
	Network inventory
Content scanning	Detecting unauthorized e-mail messages
	Checking web sites visited
Customer authorization	Registration services
	Authentication services
	Customer management services
Vulnerability analysis	Detection of vulnerabilities
	Modem detection
Intrusion detection	Intrusion detection software
Non-repudiation	Non-repudiation
Data confidentiality over networks	Policy on the use of cryptographic controls
	Data confidentiality over networks
	Key management
	Regulations of cryptographic controls
Public key infrastructure	Registration
	Key generation
	Key storage
	Certification
	Certificate revocation
	Certificate repository
	Certificate status checking
	Time-stamping
	Notarization
Network access controls	Application authentication
	Node authentication
Network access controls *(Continued)*	Mutual authentication
	Policy on use of network services
	Segregation in networks

Table G.1 — Types of control	
Identification and authentication	**User identifiers**
	Enforced path
	Remote diagnostic port protection
	Network connection control
	Network routing control
	Network firewalls
	Internet firewalls
	Publicly available systems
	Network management traffic control
	Network perimeter
	Gateway/firewall policy and procedures
Security of routing tables	Configuration of gateways, routers and bridges
	Protecting domain name servers
Physical network protection	Diagnostic and control equipment
	Distribution and termination equipment
	Protecting cabling against physical damage
Wireless LAN security	Authenticating wireless devices
	Encryption of wireless traffic
Protection of voice over IP (VOIP) traffic	Security of VOIP infrastructure
	Authentication of VOIP device
	Privacy of VOIP traffic
Message security	Submission acknowledgement
	Message origin authentication
	Delivery checking
	Security policy for electronic mail
Electronic commerce security	Electronic commerce security
Mobile code protection	Mobile code controls
Mobile code protection *(Continued)*	Controls over down-loading files
	Prevent the tracking of sites visited by users
Network resilience	Network resilience
	Network device redundancy

Table G.1 — Types of control	
Identification and authentication	**User identifiers**
	Monitoring state of network
Anti-spamming controls	Detection and control of spam messages
Protection against delay in delivery	Protecting against delays in delivery
Quality of network service	Defining quality of service
	Monitoring quality of service
Protection against denial of service attacks	Prevention of denial of service attacks
	Handling denial of service attacks
Data integrity over network	Data integrity over network
Preservation of message sequencing	Messaging sequencing
Traffic padding	Traffic padding
PBX Security	Protecting private branch exchanges
	Protecting automatic call distribution (ACD) systems
Operations controls	Operator procedures
	Operator logs
	Fault logging
	Personnel procedures
	Monitoring of activity
	Network procedures
	Network controls
	Network management
	External facilities management
System administration controls	Operational change control
	Technical review of operating system changes
	Control of access to the system managers accounts
	Restrictions on changes to software packages
Application development controls	Development standards
	Development controls
	Change control
	Authorization procedures
	Failure recovery

Table G.1 — Types of control	
Identification and authentication	**User identifiers**
Application programmer controls	Personnel procedures
	Control of operational software
	Protection of system test data
	Access control to programme source
	Access control
	Outsourced software development
Software maintenance controls	Validating identity of software maintenance engineers
	Checking software maintenance tasks
Hardware maintenance controls	Hardware maintenance procedures
	Supervision of hardware maintenance personnel
User control	User controls
Application input/output controls	Verifying the integrity of the data being input
	Output data validation
	Displaying protective marking on screen
Financial accounting	System reconciliation procedures
	Usage monitoring procedures
	Document reconciliation
	Secure destruction
	System reconciliation
	Data integrity
Hardcopy output controls	Labelling hardcopy outputs
	Hardcopy contents control
Document/media controls	Classification scheme
	Document/media labelling
Document/media controls *(Continued)*	Document/media storage
	Document/media control
	Document reproduction
	Document/media accounting
	Document/media destruction
	Automated MEDIA accounting

Table G.1 — Types of control	
Identification and authentication	**User identifiers**
	Document/media destruction facilities
	Management of removable computer media
	Information handling procedures
	Security of system documentation
Physical media transportation	Media storage during transportation
Recovery option for hosts	Recovery of hosts
Recovery options for network interfaces	Recovery of network interfaces
Recovery options for network services	Recovery of network services
Recovery options for accommodation	Recovery of accommodation
Recovery options for media	Recovery of media
Business continuity planning	Business recovery
	Business continuity and impact analysis
	Writing and implementing continuity plans
	Testing business continuity plans
	Maintaining business continuity plans
Insurance	Insurance of properties
	Insurance of equipment and stock
	Insurance against business interruption
Back-up of data	Data back-ups
	Back-up technology
Capacity planning	Capacity planning review
	Software capacity planning
	System acceptance
Equipment failure protection	Equipment failure protection
	Equipment support
	Equipment resilience
Site/building physical security	Building design
	External doors
	Staff passes
	Building entry control

Table G.1 — Types of control	
Identification and authentication	**User identifiers**
	External windows
	Building intruder detection system
	Perimeter of the site
	Security lighting
	Control of visitors
	Building monitoring
	Site monitoring
Accommodation moves	Moving items between sites
Room/zone physical security	Room design
	Controlling the distribution of keys
	Working in a secure area
Theft protection	Theft detection
	Theft prevention
Physical equipment protection	Equipment storage
	Equipment siting
Fire protection	Fire detection
	Fire evacuation
	Fire prevention
	Suppression and control
Water protection	Water control
	Water detection
	Prevention of water damage
Natural disaster protection	Asset protection
	Disaster prevention
	Lightning protection
Power protection	Installation procedures
	Power conditioning
	Power resilience
	Emergency procedures
Environmental protection	Environment protection

Table G.1 — Types of control	
Identification and authentication	**User identifiers**
	Environmental resilience
	Environmental monitoring
	Physical protection
Personnel	Recruitment screening
	Terms and conditions of employment
	Security in job descriptions
	Confidentiality agreement
	Disciplinary process
Security education and training	Security education and training
	Other forms of information exchange
Security policy	Security policy and procedures
	Review security policy
Security infrastructure	Security infrastructure
Outsourcing	Requirements in third party contracts
Data protection legislation	Data protection management structure
	Notification of processing
	Processing compliance
	Data subjects rights
	Data protection awareness training
	Reviewing of personal data and register entry
Incident handling	Security incident reporting
Incident handling *(Continued)*	Security weaknesses reporting
	Reporting software malfunctions
	Learning from incidents
	Collection of evidence
Compliance checks	Identification of applicable legislation
	Intellectual property rights (IPR)
	Compliance checks

Annex H (informative) Some particular risks

H.1 Decision support systems

H.1.1 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 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.

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. A number of such avoidable incidents involved poor or “wrong” diagnoses or other decisions. A contributing factor is often missing or incomplete information or simply ignorance, e.g. of clinical options in difficult circumstances or cross-reaction of treatments.

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

Increased decision support can be anticipated not only in clinical treatment but also in areas just as important to patient safety such as referral decision-making, where failure to make a “correct” referral or to make one “in time” can have serious consequences. Economic pressures are also leading to more decision support systems. The area of generic and/or economic prescribing is the most obvious, but economy in number and costs of clinical investigative tests is another.

Systems such as for decision support have considerable potential for reducing clinical errors and improving clinical practice, e.g. to the reduction in errors and adverse incidents resulting from the deployment of electronic prescribing. However, all such systems also carry the potential for harm. Harm can of course result from unquestioning and/or non-professional use 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:

- 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. Not least of these is the reliance a user may place on the clinical evidence that underpins decision support systems. Unless this evidence is sound at the outset and kept up-to-date with current clinical knowledge and practice, patient safety may be put at risk.

A range of example incidents, many of which relate to decision support, is provided in Annex A.

H.1.2 Risk management of 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, both during manufacture and deployment/use will be necessary to ensure the evidence and algorithms are up-to-date and that, whenever new clinical evidence emerges and is incorporated into new releases, no new risks arise. In addition, the health organization will need to ensure that access to the rules base, maintenance functions for it and the processes that use it, are correctly mapped in their organizational approach, by way of the system's access control functionality.

E-prescribing software incorporates decision support with the potential for reducing adverse clinical incidents. However, unless great care is taken in careful drug mapping/cross-mapping in the underlying reference data base, patient safety may be compromised.

Drug cross-mapping in any system can, in particular, introduce the risk of very serious errors. Risk avoidance is obviously the preferable route by eliminating cross-mapping through the use in all systems of one recognised and reputable third party drug formulary. If cross-mapping is unavoidable then automated tools should be sought rather than human, visual cross-mapping. If human, visual cross-mapping is undertaken then double checking should be undertaken.

References [37] and [38] describe the kinds of unintended consequences related to the implementation of a computerized provider order entry in decision support systems.

H.1.3 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 “Proposed next steps” [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 in to 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 Report 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 [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.2 Clinical data migration

Migration of clinical data between systems, particularly from old to new products, can be the source of serious risks which users should address carefully with a documented plan which should include:

- field level data mapping;
- specification of proper data reconciliations;
- examination of batch controls applied by the data supplier;
- examination of exception handling, etc.

Close collaborative working with any supplier of data will be important.

H.3 Time

Many aspects of clinical care and accurate record keeping depend on accuracy in the recording of time. It will be important that interoperating systems run on the same time and can cope with time changes.

H.4 Turnover of clinical staff

The turnover of clinical staff can, in some organizations, be substantial and temporary or "agency" staff may be employed in significant numbers. Where the control of risks requires action by clinical staff, this flux in staff can represent a considerable hazard. Steps will need to be taken to ensure all staff are aware of what is expected of them as soon as they are deployed in the organization.

Annex I (informative) Requirements of a clinical safety case report

I.1 Introduction

Clause 9 recommends that a health organization make available an appropriate date-stamped clinical safety case report to users of the product(s) or system.

The possible different stages of a health software system's life cycle and associated clinical safety cases or stages and clinical safety case reports are described in Clause E.2.

I.2 Structure

The clinical safety case report is the primary vehicle for presenting a statement concerning the clinical safety of the software system at a defined point in the development life-cycle.

It should provide:

- a summary of all the relevant knowledge that has been acquired relating to the clinical safety of the product up to the relevant point of the life cycle;
- a clear and concise record of the process that has been applied to determining the clinical safety of the health software system;
- a suitable summary of the outcomes of the assessment procedures applied;
- a clear listing of any residual risks that have been identified and the related operational constraints and limitations that are applicable to the ongoing maintenance of the identified residual risk at the stated level.

The clinical safety case report needs to be a single readable document rather than a complete listing of the clinical safety case or of the content of the clinical risk management file. To this end, the content of the clinical safety case report will need to cover the following minimum aspects.

- Section 1 Introduction and system description including how this safety case report relates to other interrelated systems and any wider governance arrangements.
- Section 2 Process management systems applied up to the relevant point in the life-cycle process.
- Section 3 Hazard identification and risk assessment process.
- Section 4 Applicable criteria.
- Section 5 Statement of residual risk.
- Section 6 Overall clinical safety justification.
- Section 7 References and supporting information.

Annex J (informative) **Matching resources to organizational complexity and risk**

J.1 Introduction

Health organizations vary considerably in their organizational complexity and their installed IT systems. For example, a small GP practice and a large teaching hospital obviously present substantially different challenges for risk management and consequently would require very different levels of resources and different administrative structures to undertake the risk management processes recommended in this Technical Report.

When considering the organization and resources that are necessary it will be important to keep in mind the following essential elements:

- the scope or boundary of the system that is to be subject to the risk management processes needs to be clearly defined;
- a hazard and risk identification needs to be undertaken in a formal manner with expert clinical input and the results recorded;
- an acceptable level of risk needs to be defined and recorded;
- controls need to be identified and documented to ensure risks are acceptable;
- the results of these processes need to be summarised and provided to the system users so that they can understand what has been done and what contribution they need to make, if any, to controlling risks;
- the results need to be reviewed regularly and updated in the light of experience.

J.2 Very simple configurations

A simple configuration would be a single PC running only one or a few applications which might impact on patient safety and perhaps with only one or a few users. The resource which would need to be directed at risk management in this circumstance would depend on the maximum risk which might arise. If the maximum risk is judged negligible or falls within the “acceptable” boundary then little needs to be done except to record how the maximum risk was assessed and the criteria on which it was judged acceptable (the risk management file and safety case) and to present the results to all the users (the safety case report). The identification of the maximum risk should be undertaken with some formality since systems which might at first sight seem harmless may, with a more systemized approach, be found to present risks. EN TS 15260 [10] could be used for this purpose.

Thus a single PC research system containing person-identifiable data of little or no sensitivity might readily be assessed as having a maximum risk to patient safety which is negligible and requires no significant controls. However if the research system contained person-identifiable data about, for example, sexually transmitted diseases, there would be hazards from breaches of confidentiality and consequent psychological harm to patients and the risks to be controlled would involve all users being aware of, and conforming to, good security practices.

J.3 More complex configurations, e.g. small GP practices

For a small GP practice with just two or three networked PCs, delineating the system boundary will be relatively straightforward although some thought will need to be given to how to deal with the interface between the GP practice IT and the “outside” world, e.g. communication to and from local hospitals, other GPs, the internet etc. Expertise will be required in hazard and risk identification and risk control and this may need to be brought in since it may not be available in house. However, as a starting point, it will often be possible to get access to the results from other practices with similar configurations [e.g. from the system supplier(s)] and the supplier(s)/manufacturer(s) should be asked for a safety case report or equivalent. These will greatly simplify matters although care needs to be taken to check that the results from others are genuinely mirrored. Clinical input to the risk management processes can come from the practice's GPs being given some basic training.

The documentation from the process will comprise the risk management file and the analysis and controls, if properly structured, will become the safety case. A summary of what has been done with clear delineation of any administrative control measures which the users (the GPs) need to undertake will comprise the safety case report. The major task will be undertaking this process for the first time. Thereafter, the process should become easier and will focus on matters such as system updates and patches from the supplier(s). The latter should be required to provide safety case updates as appropriate which should include the supplier's assessment of any impact on the customer from new or changed risks if any.

There are a variety of arrangements which a GP practice might make with IT suppliers and IT support organizations. Whatever the arrangement, clear lines of responsibility need to be established and documented. Thus, where, for example, an external organization is responsible for installing updates, patches, maintenance activities etc., the associated responsibility for risk management should also be defined. Where the external body is responsible there should be a requirement to maintain the associated safety case and to provide safety case update reports whenever risk changes.

Software often allows the customer to undertake local configuration and customization. The practice will need to take responsibility for risk management in this respect. Systems will often incorporate decision support from which particular and potentially serious risks could arise (see Annex H) and assurances from the system manufacturer should be sought about the adequacy of their risk control measures. The hazards that can arise from data migration, definitional or coding/classification changes and the import of data/patient records from other practices or sources should receive particular attention.

As always, serious attention needs to be given to hazards arising from hackers, viruses and other attacks, threats to confidentiality, system downtime or crashes, internal networks, backup provisions and other security matters. Controlling threats to confidentiality will in particular involve administrative measures affecting all users.

J.4 Complex configurations, e.g. hospitals

Complex configurations, for example as found in most hospitals, will require the harnessing of significant expert resources. Nevertheless, given some training in risk management, most of this should be available internally, e.g. clinical expertise and information management and IT expertise. This resource will, however, need to be brought together into a suitable organizational structure. The “responsible person” in

charge of patient safety and in overall control of the risk management process will need in-depth knowledge and experience of risk management techniques. Top management will need to be formally engaged.

Starting from scratch, the first challenge will be to carefully define the software system boundaries and the nature of the interfaces between the defined system (which may contain several software products) and systems outside the boundary. Compartmentalizing a complex system of interoperating products into a system of systems, is challenging and understanding the relationships between components will be essential. It will be useful to remember that the compartmentalization is for the purpose of hazard and risk identification and the control/mitigation of those risks and may therefore not coincide with other boundaries such as departments or specialities or particular applications. As the risk management process is applied within each defined boundary within a system of products or applications, it will be necessary to undertake iterative reviews to see whether one analysis impacts on another. Deciding where to start and what products and systems to address first may be assisted by crudely “classifying” products/systems according to the maximum seriousness of the risk they may pose to patients such as described in EN TS 15260 [10].

In an ideal world, the starting point for any risk analysis would be the clinical safety case reports from the manufacturers of each of the products involved within the defined system boundary, i.e. the “output” from manufacturers applying ISO/TS 29321. However until that Technical Specification is widely applied such reports may not be available for products already in place. Customers should therefore require compliance with ISO/TS 29321 when buying new products. If clinical safety reports are not available from a manufacturer then the health organization's own clinical safety case will need to be built from scratch through the application of this Technical Report (whose processes are substantially the same as ISO/TS 29321).

An essential starting point will be:

- a corporate data model encompassing both clinical and administrative data sets;
- application architecture diagrams;
- network topology.

It is likely that the organization will have a number of shared infrastructure components/servers such as staff and access directories, master patient index, common clinical and administrative data sources, coding/classification directories, messaging support functions. These will be good starting points before moving to the applications which rely on them. This would similarly apply to technical infrastructure components such as:

- network(s);
- protected power supplies;
- printer infrastructures;
- common hardware components;
- backup storage;
- identity management;
- access management.

Bibliography

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

[2] An Organization with a Memory, HMSO, June 2000

[3] Quality in Australian Healthcare, Study, 1994

[4] BRENNAN, T.A., LEAPE, I.I., LAIRD, N.M., HERBERT, I., LOCALIO, A.R. and LAWTHERS, A.G. Incidents of adverse events and negligence in 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.GRAMM.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] IEC 80001, Working Draft 1, Application of risk management to information technology (IT) networks incorporating medical devices, 15th March 2007

[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] ISO/TS 29321:2008, Health informatics — Application of clinical risk management to the manufacture of health software In draft check publication reference number and year before publication

[34] ISO 20856, Health Informatics — Security management in health using ISO/IEC 17799

[35] 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

[36] 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

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

[38] 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

