Document filename: **SCCI0129 Implementation Guidance v3.1**			
Directorate	**Solution Design Standards and Assurance**	Project	**Clinical Safety**
Document Reference		**NPFIT-FNT-TO-TOCLNSA-1300.05**	
Director	**Debbie Chinn**	Status	**Approved**
Owner	**Stuart Harrison**	Version	**3.1**
Author	**Frazer Brindley** **Sean White**	Version issue date	**16.08.2016**

Clinical Risk Management: its Application in the Manufacture of Health IT Systems - Implementation Guidance

Document Management

Revision History

Version	Date	Summary of Changes
0.1	16.11.2012	First draft
0.2	10.12.2012	Revised following review by external appraisal. For approval
1.0	03.01.2013	First issue
1.1	17.01.2013	Incorporation of changes following review by Information Standards Management Services. For approval
2.0	21.01.2013	Approved
2.1	09.05.2013	HSCIC rebranded, correction to Figure A and additional paragraph added to section 4.3
3.0	08.12.2105	Amended and Approved to reflect changes made to Requirement 2.5
3.1	16.08.2016	NHS Digital Rebranded

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
	NHS Digital Clinical Safety Group	16.08.2016	3.1
Deborah Raven	Information Standards Management Services	17.01.2013	1.0

Approved by

This document must be approved by the following people:

Name	Title	Date	Version
Dr Sebastian Alexander	Interim Clinical Director for Patient Safety	16.08.2016	3.1
Debbie Chinn	Director of Solution Assurance	16.08.2016	3.1

SCCI Standardisation Committee for Care Information

This information standard (SCCI0129) has been approved for publication by NHS England under section 250 of the Health and Social Care Act 2012.

Assurance that this information standard meets the requirements of the Act and is appropriate for the use specified in the specification document has been provided by the Standardisation Committee for Care Information (SCCI), a sub-group of the National Information Board.

This information standard comprises the following documents:

- Specification
- Implementation Guidance.

An Information Standards Notice (SCCI0129 Amd 39/2012) has been issued as a notification of use and implementation timescales. Please read this alongside the documents for the standard.

The controlled versions of these documents can be found on the SCCI webpages

Date of publication: 5 May 2016 (documents updated 16 August 2016 to reflect the adoption of NHS Digital as the trading name of the Health and Social Care Information Centre).

Related Documents:

These documents provide additional information and are specifically referenced within this document.

Ref	Doc Reference Number	Title	Version
1.	ISB 0160 (DSCN 18/2009)	Guidance on the management of clinical risk relating to the Deployment and Use of Health Software: www.isb.nhs.uk/library/standard/162	2009
2.	SCCI0160 Amd 38/2012	Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems: www.digital.nhs.uk/isce/publication/scci0160	4.1
3.	ISB 0129 (DSCN 14/2009)	Application of Patient Safety Risk Management to the Manufacture of Health Software: www.isb.nhs.uk/library/standard/163	2009
4.	SCCI0129 Amd 39/2012	Clinical Risk Management: its Application in the Manufacture of Health IT Systems: www.digital.nhs.uk/isce/publication/scci0129	3.1
5.	2007/47/EC	Medical Device Regulations (amendment 2010)	
6.	ISO 14971:2009	Medical Devices: Application of Risk Management to Medical Devices	2009
7.		ALARP (HSE Website)	
8.		2006 Annual Report of the Chief Medical Officer On the State of Public Health, Department of Health	2006
9.	0555	Healthcare risk assessment made easy, NPSA	2007
10.	NPFIT-FNT-TO-TOCLNSA-1170	DSCN 14/2009 and DSCN 18/2009 Implementation Review	2012
11.		Managing competence for safety-related systems, HSE	2007

Contents

1 Introduction

1.1 Background

The provision and deployment of Health IT Systems within the National Health Service (NHS) can deliver substantial benefits to NHS patients through the timely provision of complete and correct information to those healthcare professionals that are responsible for administering care. However, it must be recognised that failure, design flaws or incorrect use of such systems has the potential to cause harm to those patients that the system is intending to benefit.

An assessment on the effectiveness of the implementation of ISB 0160 [Ref. 1] was carried out during 2011 as part of its normal maintenance cycle. Based on the results of this assessment [Ref. 10], the standard was revised to provide a simpler and more structured document; where the clinical risk management requirements were separated from the guidance material [Ref. 2].

As the clinical risk management requirements for Manufacturers are very similar to the requirements for Health Organisations, it was considered appropriate to revise ISB 0129 [Ref. 3]. The impact of the recent changes in the NHS reform has also been considered within the revision.

This document provides guidance to support the interpretation of the requirements presented in SCCI0129 [Ref. 4]. It is aimed at those persons within a Manufacturer's organisation who are responsible for ensuring the safety of Health IT Systems through the application of clinical risk management. To aid readability, the structure of this guidance document mirrors that of the revised standard; where each requirement is presented and then supported by additional information.

Whereas this document is restricted to Health IT Systems, the recommended risk analysis should be conducted within the context of any overall risk management system in place in the Manufacturer's organisation and any wider health information governance processes. In this document the term 'clinical risk' is used to make clear that its scope is concerned with risks to patient safety as distinct from other types of risk such as financial.

Throughout this guidance the term 'standard' is used to specifically mean SCCI0129 [Ref. 4]. Within this document the term 'should' does not infer any additional requirements to those explicitly taken from the standard (as shown in capital letters).

1.2 Scope

This guidance document considers the risk management processes required to ensure patient safety in respect to the development of a new Health IT System or in respect to the modification of an existing system.

A Health IT System is defined as a product used to provide electronic information for health or social care purposes where the product may include hardware, software. or a combination of both. The scope of the Health IT System may extend beyond a Manufacturer's organisation and include hardware and or software procured or supplied from other organisations and include infrastructure already in use at a Health Organisation. Further guidance is presented at Section 2 and in Figure B.

The scope of a specific Health IT System will therefore need to be defined by a Manufacturer as part of the early lifecycle phases, possibly in conjunction with the Health Organisation.

This document is addressed to those persons in the Manufacturer's organisation who are responsible for ensuring the safety of Health IT Systems through the application of risk management.

In the development and modification of a Health IT System, the scope of the standard and this supporting guidance includes:

- all clinical functionality which could potentially cause harm to patients
- operational use and potential misuse of the clinical functionality and its potential to cause harm to patients.

This standard applies to Health IT Systems that are not controlled by medical device regulations [Ref. 5], though the requirements are broadly consistent with the requirements of ISO 14971 [Ref. 6].

A Manufacturer will need to identify which other standards are applicable to the development of the Health IT System. Compliance to such standards is, however, out of the scope of SCCI0129.

1.3 Glossary of terms

Term	Definition
Clinical Safety Officer (previously referred to as Responsible Person)	Person in a Manufacturer's organisation responsible for ensuring the safety of a Health IT System in that organisation through the application of clinical risk management.
Clinical risk	Combination of the severity of harm to a patient and the likelihood of occurrence of that harm.
Clinical risk analysis	Systematic use of available information to identify and estimate a risk.
Clinical risk control	Process in which decisions are made and measures implemented by which clinical risks are reduced to, or maintained within, specified levels.
Clinical risk estimation	Process used to assign values to the severity of harm to a patient and the likelihood of occurrence of that harm.
Clinical risk evaluation	Process of comparing a clinical risk against given risk criteria to determine the acceptability of the clinical risk.
Clinical risk management	Systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling clinical risk.
Clinical Risk Management File	Repository of all records and other documents that are produced by the clinical risk management process.
Clinical Risk Management Plan	A plan which documents how the Manufacturer will conduct clinical risk management of a Health IT System.
Clinical Risk Management Process	A set of interrelated or interacting activities, defined by the Manufacturer, to meet the requirements of this standard with the objective of ensuring clinical safety in respect to the development and modification of a Health IT System.
Clinical safety	Freedom from unacceptable clinical risk to patients.
Clinical Safety Case	Accumulation and organisation of product and business process documentation and supporting evidence, through the lifecycle of a Health IT System.
Clinical Safety Case Report	A Report that presents the arguments and supporting evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment at a defined point in a Health IT System's lifecycle.
Harm	Death, physical injury, psychological trauma and/or damage to the health or well-being of a patient.
Hazard	Potential source of harm to a patient.
Hazard Log	A mechanism for recording and communicating the on-going identification and resolution of hazards associated with a Health IT System.
Health Organisation	Organisation within which a Health IT System is deployed or used for a healthcare purpose.
Health IT System	Product used to provide electronic information for health or social care purposes. The product may be hardware, software or a combination.
Initial clinical risk	The clinical risk derived during clinical risk estimation taking into consideration any retained risk control measures.

Term	Definition
Intended use	Use of a product, process or service in accordance with the specifications, instructions and information provided by the manufacturer to customers.
Issue	The process associated with the authoring of a document. This process includes: reviewing, approval and configuration control.
Likelihood	Measure of the occurrence of harm.
Lifecycle	All phases in the life of a Health IT System, from the initial conception to final decommissioning and disposal.
Manufacturer	Person or organisation with responsibility for the design, manufacture, packaging or labelling of a Health IT System, assembling a system, or adapting a Health IT 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.
Patient	A person who is the recipient of healthcare.
Patient safety	Freedom from harm to the patient.
Post-deployment	That part of the lifecycle of a Health IT System after it has been manufactured, released, deployed and is ready for use by the Health Organisation.
Procedure	Specified way to carry out an activity or a process.
Process	Set of interrelated or interacting activities which transform inputs into outputs.
Release	A specific configuration of a Health IT System delivered to a Health Organisation by the Manufacturer as a result of the introduction of new or modified functionality.
Residual clinical risk	Clinical risk remaining after the application of risk control measures.
Safety incident	Any unintended or unexpected incident which could have, or did, lead to harm for one or more patients receiving healthcare.
Safety Incident Management Log	Tool to record the reporting, management and resolution of safety incidents associated with a Health IT System.
Severity	Measure of the possible consequences of a hazard.
Third party product	A product that is produced by another organisation and not by the Health IT System manufacturer. Examples include operating systems, library code, database and application servers and network components.
Top Management	Person or group of people who direct(s) and control(s) an organisation and has overall accountability for a Health IT System.

2 General requirements for clinical risk management

In the manufacture of a Health IT System, clinical risk management is an essential activity in ensuring the system does not compromise patient safety. The focus for a Manufacturer should be on ensuring that the Health IT System they deliver does not introduce unnecessary clinical risk and wherever possible reduces existing clinical risk.

General requirements for effective clinical risk management are:

- an understanding of the hardware/software and underlying development practices being used to implement the Health IT System
- a thorough understanding of:
  - the clinical functionality that the Health IT System is intending to provide or replicate
  - the business processes that the Health IT System is intending to support
  - usability issues which may result in unintended consequences to patients
- assessment of any known deficiencies in existing systems or business processes
- an appropriate awareness of clinical risk management
- an awareness of how clinical risk management aligns with any wider governance processes
- a fully defined clinical risk assessment process which incorporates the application of recognised and rigorous methodologies (for example, see Appendix B)
- a risk assessment to be carried out completely and competently
- the implementation and verification of any required clinical risk control measures
- any residual clinical risks are appropriately documented
- appropriate lifecycle management is in place.

Figure A presents a pictorial summary of the end-to-end clinical risk management process including the activities and documentation as required by the Standard.

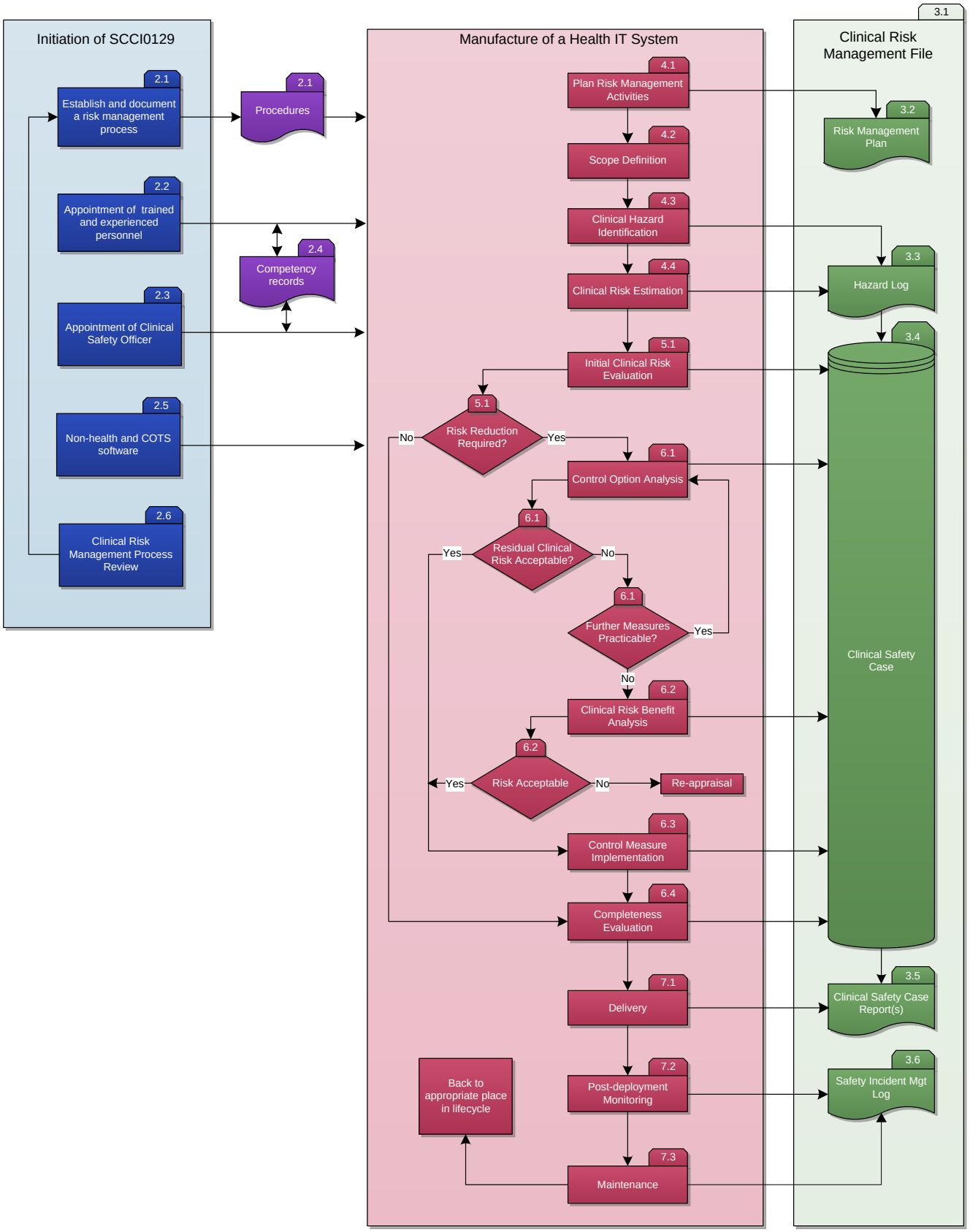

Figure A Clinical Risk Management Activities and Documentation

The term Manufacturer is used to cover all organisations which are involved in the development of some aspect of a Health IT System. In this respect, Manufacturer is inclusive of terms such as: provider, integrator, supplier, developer, vendor, etc.

Manufacturers which are including software or hardware procured from other Manufacturers, must assure themselves of the suitability of these items. Ideally, such components should be manufactured in accordance with SCCI0129 and be accompanied by appropriate safety documentation. It is, however, recognised that certain components such as third party products will not fall under this definition; see section 2.5. Here the Manufacturer is to take reasonable steps, based on perceived risks, to assure itself that the inclusion of such products does not pose an unacceptable risk to patient safety. Where a Manufacturer uses components that do not have the necessary safety documentation, then the Manufacturer will also be responsible for undertaking and documenting an appropriate assessment of the component concerned as part of his wider offering.

An example procurement chain for a new Health IT System is depicted In Figure B. Within this example, the Manufacturer responsible for the delivery of the Health IT System (Manufacturer B) to the Health Organisation has integrated:

- third party product
- Health IT System A which implements specific functionality (purchased from Manufacturer A)
- software internally developed.

This integrated software has then been installed on to a procured general hardware platform. *Note, none of the elements in this figure are considered to be a medical device.*

The delivered third party products (software and hardware) from their respective vendors are not accompanied by any supporting safety documentation. As a result, Manufacturer B is required under requirement 2.5 of SCCI0129 to assure itself that any clinical hazards arising from these components are suitably addressed.

As Health IT System A from Manufacturer A has been specifically developed to implement health functionality it meets the requirements of SCCI0129. Its delivery is therefore accompanied by a Clinical Safety Case Report. This Clinical Safety Case Report has then been referenced by an overall Clinical Safety Case Report produced by Manufacturer B to accompany the release of Health IT System B. Both of these Clinical Safety Case Reports have been provided to the Health Organisation.

In the following sections the requirements as presented in the standard are reproduced to aid readability. Each requirement is shown in a coloured table along with the original reference number.

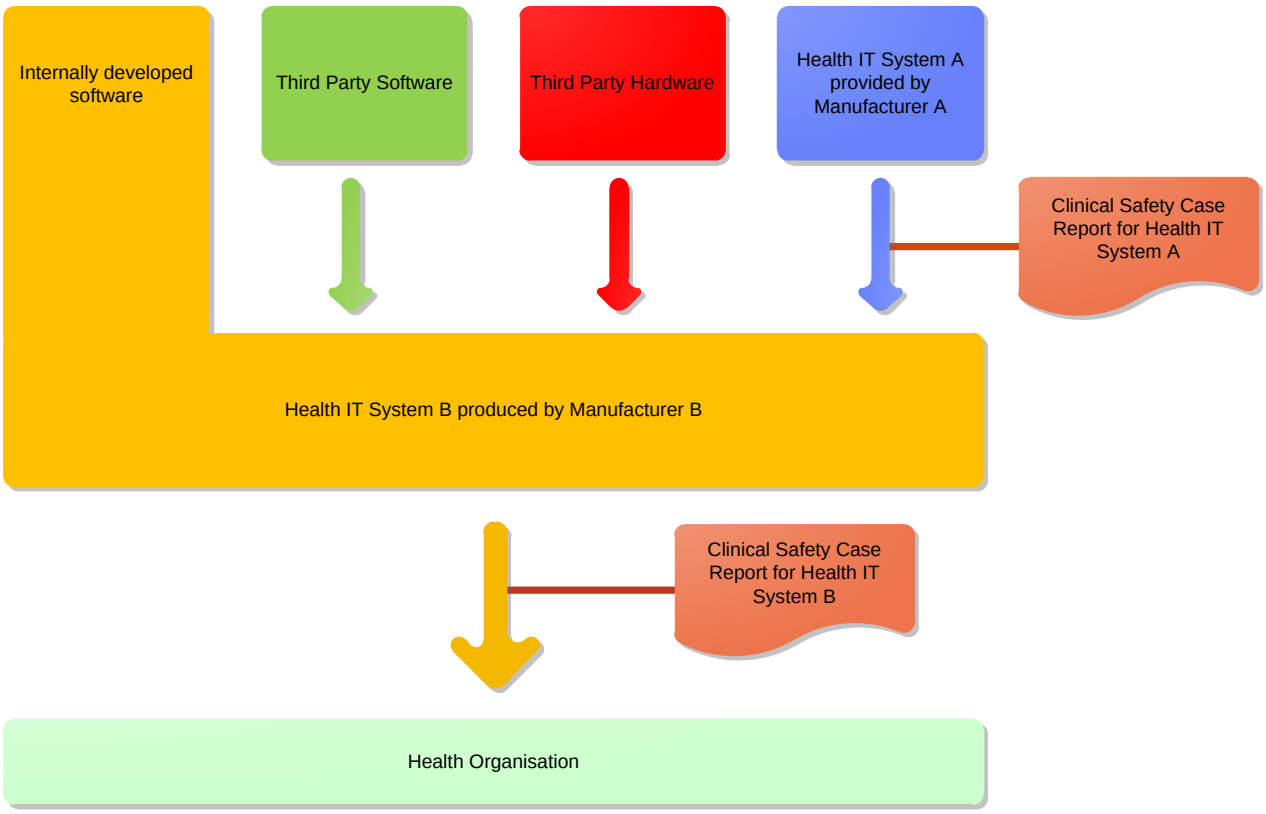

Figure B Health IT System procurement and documentation chain

2.1 Clinical risk management process

2.1.1	The Manufacturer MUST define and document a clinical risk management process which recognises the risk management activities shown in Figure 1. *Note: the numbers shown in parentheses in this figure refer to sections later in this document.*

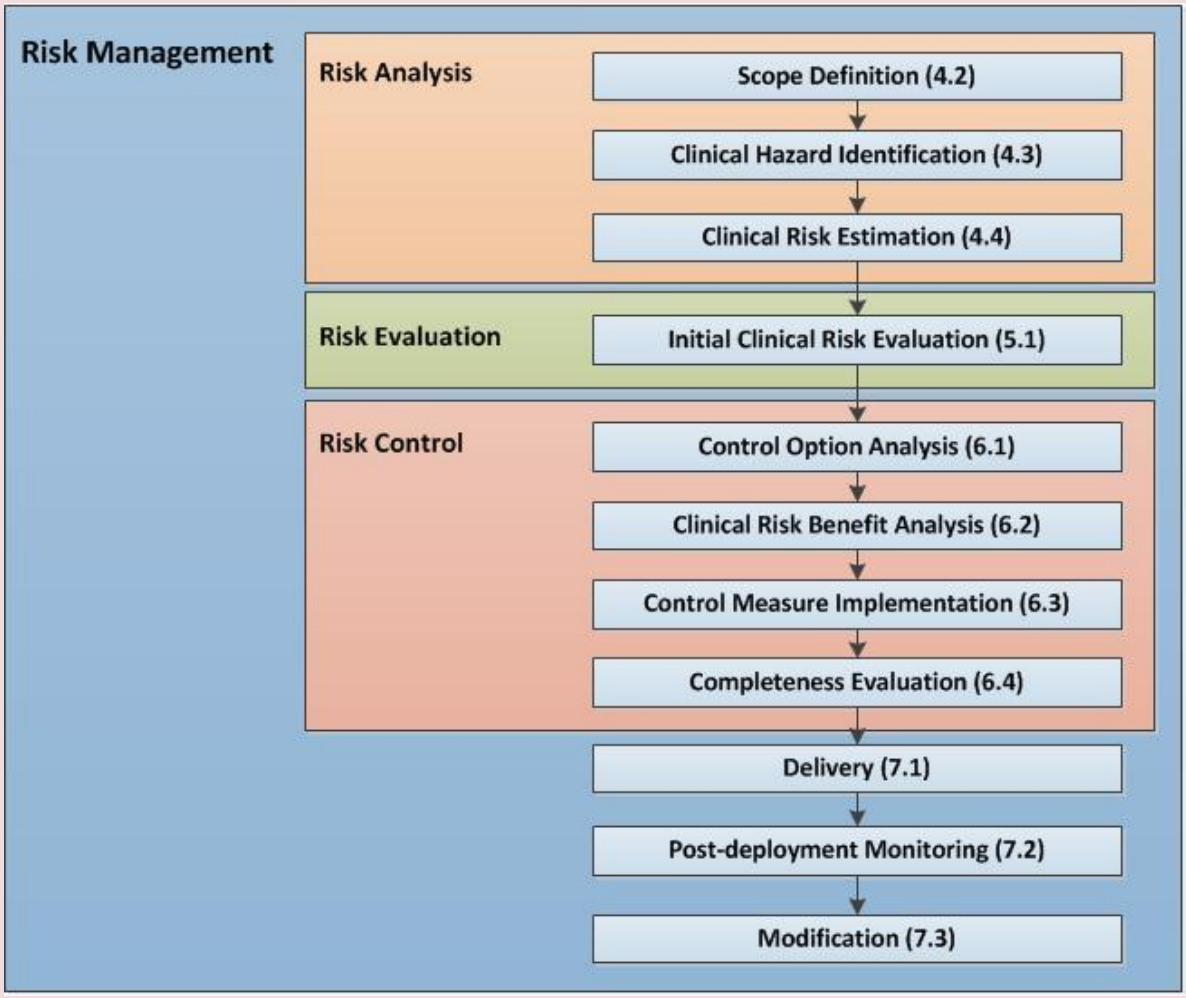

Figure 1 Clinical Risk Management Process

In order to ensure that the clinical risk analysis is performed in a structured and comprehensive manner the Manufacturer needs to define and document its clinical risk management process. The process is expected to cover the development and maintenance phases of the lifecycle of any Health IT System impacted by this standard.

The clinical risk management process will recognise the activities shown in Figure 1. Further detail on each activity and associated requirements can be found by referring to the referenced section of this guidance document.

This process can be conducted within the context of the organisation's wider risk management policies, quality management system and any governance arrangements, e.g. for information/health informatics.

The same clinical risk management process may not be appropriate for all releases; definitions of risk acceptability criteria, hazard severity and likelihood may vary across Health IT Systems. The Manufacturer is responsible for ensuring the clinical risk management process is applicable to a given release. Prior to tailoring the clinical risk management process, the Manufacturer will, as far as is reasonably practical, require an understanding of the system to be deployed and how it will be used.

Strong co-operation between the Manufacturer and the Health Organisation throughout the clinical risk activities is encouraged, where possible, if the clinical risk associated with the deployment of a Health IT System is to be minimised.

2.2 Top Management responsibilities

2.2.1	In implementing the clinical risk management process for a given deployment, Top Management MUST: • make available sufficient resources • assign competent personnel (see section 2.4) from each of the specialist areas that are involved in developing and assuring the Health IT System • nominate a Clinical Safety Officer.
2.2.2	Top Management MUST ensure that appropriate levels of authorisation for the Health IT System and its safety documentation are defined in the Clinical Risk Management Plan.

The extent of clinical risk analysis and hence the level of resources required to support the process will need to be commensurate with the scale, complexity and level of clinical risk associated with the release.

The assessment of the required resources may be guided by experience from previous developments, including input from personnel involved in those developments. The level of resource required would also be dependent on the Health IT System development timescales.

The nominated resources need to have sufficient time available to allow them to apply a suitable level of effort to ensure the clinical risk management process is completed in a robust and competent manner. Such personnel will be able to contribute their specialist knowledge to ensure the clinical risk management activities are executed as competently and completely as possible. A list of typical specialist areas that may be required to support clinical risk activities can be seen in section 4.1 of this guidance document.

The roles and responsibilities of personnel supporting the clinical risk management activities will need to be documented in the Clinical Risk Management File.

A Clinical Safety Officer has to be nominated for a given release. The Clinical Safety Officer will be responsible for ensuring the safe design of a Health IT System through the application of the clinical risk management process. The nominated Clinical Safety Officer needs to satisfy the requirements of section 2.3 of the standard.

Top Management remains responsible for identifying who in the Manufacturer organisation is responsible for authorising the release of the Health IT System for subsequent use in live service. This needs to be recorded in the Clinical Risk Management Plan.

Within the Clinical Risk Management Plan, Top Management will need to specify those individuals who are able to approve the clinical risk management documentation. As a minimum this will be the Clinical Safety Officer.

The Manufacturer needs to undertake a formal review of the clinical risk management activities (see section 4.1) prior to the release of a Health IT System. The outcome of this review will be a key input into this Top Management decision making process.

Top Management will need to satisfy itself that all foreseeable hazards have been identified and that the risk of such hazards has been reduced to acceptable levels. By authorising the release of the Health IT System, Top Management is accepting any residual clinical risk on behalf of the Manufacturer.

2.3 Clinical Safety Officer

2.3.1	A Clinical Safety Officer MUST be a suitably qualified and experienced clinician.
2.3.2	A Clinical Safety Officer MUST hold a current registration with an appropriate professional body relevant to their training and experience.
2.3.3	A Clinical Safety Officer MUST be knowledgeable in risk management and its application to clinical domains.
2.3.4	A Clinical Safety Officer MUST make sure that the processes defined by the clinical risk management process are followed.

The Clinical Safety Officer needs to be suitably trained and qualified in risk management or have an understanding in principles of risk and safety as applied to Health IT Systems. A Clinical Safety Officer needs to have completed appropriate training. Whilst suitable training is provided by NHS Digital in partnership with other bodies it is recognised that there are other methods to acquire relevant skills, e.g. Masters modules in Patient Safety. It would be beneficial for a Clinical Safety Officer to have experience of conducting clinical risk management activities in an appropriate clinical setting.

Table 1 summarises competencies for a Clinical Safety Officer. The table details the relevant experience, knowledge and skills that the candidate should have together with an explanation of why these are required.

Whilst some activities may be delegated, the Clinical Safety Officer will retain overall responsibility for the following activities:

- approval of the Clinical Risk Management Plan to confirm that the plan is appropriate and achievable in the context of the Health IT System development and modification
- ensure that clinical risk management activities are completed in accordance with the Clinical Risk Management Plan
- review and approval of all safety documentation including Clinical Safety Case Reports and Hazard Logs
- review of evidence in the Clinical Risk Management File to ensure it is complete and supports the Clinical Safety Case Report
- provide recommendation to Top Management regarding whether the Health IT System is safe to release
- raise any unacceptable safety risks to Top Management.

COMPETENCY	RATIONALE
EXPERIENCE	
Relevant clinical experience	A thorough understanding of the practice of related healthcare, clinical workflow and supporting business processes is required in order to understand how and why adverse outcomes occur in patients and to pre-empt potential hazards associated with the Health IT System.
KNOWLEDGE	
In depth knowledge of the Health IT System being developed, human factors and their contribution and control in the context of patient harm.	A thorough understanding of why and how errors occur in the development, deployment and subsequent use of Health IT Systems and how these can result in patient harm. Knowledge is required of measures that can be effectively applied to control associated clinical risk.
SKILLS	
Critical appraisal and logical reasoning	Must be able to independently recognise potential defects in the inherent design of a system, how unintentional errors may occur and how the system impacts existing business processes, etc. Needs to be able to critically analyse recommendations made by other representatives. Will have to make calculated decisions on whether proposed solutions are warranted and cost-effective.
Problem solving	For reported defects, must be able to identify the root cause and propose practical and effective solutions from a clinical perspective.
Ability to facilitate consensus	Must be able to consider and review differing opinions and broker the optimum solution between involved stakeholders.

Table 1 Key Competencies for a Clinical Safety Officer

2.4 Competencies of personnel

2.4.1	Personnel MUST have the knowledge, experience and competencies appropriate to undertaking the clinical risk management tasks assigned to them.
2.4.2	Competency and experience records for the personnel involved in performing the clinical risk tasks MUST be maintained.

The Manufacturer needs to use multi-discipline teams appropriate to the level of risk for the project. Evidence that the personnel have the required skill set to perform the clinical risk management tasks assigned to them can be ascertained from the individual's competency and experience records. Any shortfalls need to be identified and addressed using the Manufacturer's competency framework.

Competency and experience records for personnel involved in the clinical risk activities need to be maintained in line with the Manufacturer's Human Resource process. The records need to be reviewed and updated on a regular basis. Any new skills, training or knowledge gained as part of continued professional development needs to be added to the records to ensure that the latest information is available.

Additional guidance can be found in "Managing competence for safety-related systems" published by the HSE [Ref. 11].

2.5 Third party products

2.5.1	The Manufacturer MUST assess any third party product that is included within a release as part of the clinical risk management process.
2.5.2	The nature of this assessment MUST be included in Clinical Safety Case Reports.

Many Health IT Systems are reliant on the use of third party products. Such products can introduce a variety of risks particularly where a Health IT System is reliant upon it or interoperates with it. Risks may also arise when software updates or patches are applied to these products. Such products are, however, unlikely to have been risk assessed for health applications by the original supplier.

Manufacturers are required as part of their clinical risk assessment activities to consider any third party product incorporated into their Health IT System. The Manufacturer needs to:

- document the assessment of third party products in their Clinical Safety Case Report
- assess any changes in third party products. The Safety Case report will need to be re-issued if a change in the level of risk results.

2.6 Regular clinical risk management process review

2.6.1	The Manufacturer MUST formally review its clinical risk management process at planned, regular intervals.

The clinical risk management process needs to be formally reviewed, to ensure the process remains effective. Such a review will need to encompass representatives of the key stakeholder communities and especially the relevant clinical staff including the Clinical Safety Officer. An annual review is recommended.

The review should examine whether any changes are needed as a result of greater experience, best practice or lessons learnt from other releases to support a process of continual improvement. Any changes to the clinical risk management process may also need to be captured in any current Clinical Risk Management Plans.

Detailed records of the formal review and its findings should be retained by the Manufacturer in accordance with their management processes.

3 Project Safety Documentation and Repositories

All clinical risk documentation needs to be subject to configuration control so that any subsequent changes can be tracked.

3.1 Clinical Risk Management File

3.1.1	The Manufacturer MUST establish at the start of a project a Clinical Risk Management File for the Health IT System.
3.1.2	The Clinical Risk Management File MUST be maintained for the life of the Health IT System.
3.1.3	All formal documents and evidence of compliance with the requirements of this standard MUST be recorded in the Clinical Risk Management File.
3.1.4	Any decisions made that influence the clinical risk management activities undertaken MUST be recorded in the Clinical Risk Management File.

The purpose of the Clinical Risk Management File is to provide a physical or logical repository of all records and documents that are produced by the clinical risk management process and required by this standard. If the documents are referenced from the Clinical Risk Management File then they must be capable of being retrieved.

Consideration should be given to ensuring adequate back-up or archiving procedures are in place to ensure that the Clinical Risk Management File, and the artefacts it contains or references, remains preserved and recoverable throughout the life of the Health IT System.

3.2 Clinical Risk Management Plan

3.2.1	The Manufacturer MUST produce at the start of a project a Clinical Risk Management Plan, which will include risk acceptability criteria, for the new Health IT System.
3.2.2	A Clinical Safety Officer MUST approve the Clinical Risk Management Plan.
3.2.3	If the nature of the project changes, or key people change, during the development and modification of a Health IT System, then the Clinical Risk Management Plan MUST be updated.
3.2.4	The Clinical Risk Management Plan MUST be maintained throughout the life of the Health IT System.

The purpose of the Clinical Risk Management Plan is to document and schedule the clinical risk management activities to support the safe development and maintenance of the Health IT System.

The Clinical Risk Management Plan should:

- define and describe the Health IT System and the clinical context in which it will be used. Where the clinical context is not known, e.g. a new Health IT System, then assumptions made regarding its anticipated usage need to be recorded

- state the relevant procedures, policies and resources required to ensure effective and efficient clinical risk management
- adhere to the Manufacturer's quality and project management processes and requirements
- define the Health IT System development lifecycle and its associated phases
- qualify which clinical risk activities are applicable at a particular lifecycle phase
- specify the criteria that are to be used to estimate the clinical risk (see section 4.4) and evaluate the acceptability of the clinical risk (see section 5.1)
- identify key roles of responsibility and authority for each clinical risk activity. Additionally it needs to also identify what other resources are required to support the activity, e.g. reviewer, subject matter expert, test analyst, etc.
- define those members of staff who are able to approve the safety documentation
- record under what circumstance or periodicity the plan should be reviewed. Triggers could be at a transition to the next phase in the Health IT System lifecycle, a change of resource or in line with existing governance arrangements. The motivation for review is to maintain an up to date and effective plan and to support a process of continual improvement
- describe the process that will be used to monitor and react to safety incidents should they arise following delivery of a release of a Health IT System.

Where some of the above aspects are addressed in other management documentation, e.g. a Clinical Safety Management System, then the Clinical Risk Management Plan may reference out to such documentation.

The extent of the Clinical Risk Management Plan needs to be commensurate with the scale and clinical functionality of the Health IT System being developed whilst addressing the clinical risk management activities specified within this standard.

Both the clinical risk management and overall programme level activities need to be integrated correctly. Careful consideration needs to ensure that activities are scheduled in the correct order as certain activities may have a dependency on another. For example, Clinical Risk Control Option Analysis (section 6.1) should be completed before the Manufacturer finalises its training material; the rationale being that specific training requirements may be identified as clinical risk controls.

The Clinical Risk Management Plan needs to be approved by the Clinical Safety Officer prior to use. The Clinical Safety Officer shall have the appropriate clinical experience and risk management expertise to assess whether the plan is appropriate and achievable in the context of the Health IT System being developed and released.

The Clinical Risk Management Plan forms part of the Clinical Risk Management File.

3.3 Hazard Log

3.3.1	The Manufacturer MUST establish and maintain a Hazard Log.
3.3.2	A Clinical Safety Officer MUST approve each version of the Hazard Log.
3.3.3	An issued Hazard Log MUST accompany each Clinical Safety Case Report.

The Hazard Log is a mechanism for recording and communicating the on-going identification and resolution of hazards associated with the Health IT System. It is organised so that it enables a systematic approach to the management of hazards and supports the effective collation of safety case evidence. Such on-going revisions will:

- incorporate new hazards, when identified
- record the mitigation of defined hazards through the implementation of clinical risk control mechanisms
- reference supporting evidence
- record the status of actions.

Whilst the Hazard Log is a living document and continues to be updated during the lifecycle of the Health IT System, a base-lined version is to be issued with each Clinical Safety Case Report.

Each version of the Hazard Log has to be reviewed and approved by the Clinical Safety Officer to signify that the clinical safety information recorded is accurate and appropriate.

An example Hazard Log template is presented at Table 2. It is not prescriptive or definitive but illustrates how, reading from left to right, a well-structured Hazard Log supports effective clinical risk management and promotes the collection of relevant evidence in a timely manner. Where clinical risk control is transferred to the Health Organisation, this shall be clearly identified in the Hazard Log. In this situation, the Health Organisation will be responsible for implementing the necessary clinical risk control measures.

Additional examples are presented in Table 3 and Table 4 which illustrate how such a log would be populated for hazards with single or multiple causes respectively. Table 5 summarises the entries that are recorded in each column of a Hazard Log.

Hazard Number	Hazard Name	Hazard Description	Potential Clinical Impact	Possible Causes	Existing Controls	Initial Hazard Risk Assessment			Additional Controls				Residual Hazard Risk Assessment			Actions		Hazard Status
						Severity	Likelihood	Risk Rating	Design	Test	Training	Business Process Change	Severity	Likelihood	Risk Rating	Summary	Owner	
1																		
2																		
3																		

Table 2 Representative Hazard Log Template

Hazard Number	Hazard Name	Hazard Description	Potential Clinical Impact	Possible Causes	Existing Controls	Initial Hazard Risk Assessment			Additional Controls				Residual Hazard Risk Assessment			Actions		Hazard Status
						Severity	Likelihood	Risk Rating	Design	Test	Training	Business Process Change	Severity	Likelihood	Risk Rating	Summary	Owner	
1	X	X	X	X	X	X	X	X	?	?	?	?	X	X	X	X	X	X

Table 3 Representative Hazard log with Single Cause

Hazard Number	Hazard Name	Hazard Description	Potential Clinical Impact	Possible Causes	Existing Controls	Initial Hazard Risk Assessment			Additional Controls				Residual Hazard Risk Assessment			Actions		Hazard Status
						Severity	Likelihood	Risk Rating	Design	Test	Training	Business Process Change	Severity	Likelihood	Risk Rating	Summary	Owner	
2	X	X	X			X	X	X					X	X	X			X
				1	X				?	?	?	?				X	X	
				2	X				?	?	?	?				X	X	
				3	X				?	?	?	?				X	X	

Table 4 Representative Hazard Log with Multiple Possible Causes

X – Field to be populated

? – Field to be populated as applicable

Field	Description
Hazard number	A unique number for the hazard
Hazard name	A short descriptive name for the hazard
Hazard description	A short description of the hazard
Potential Clinical Impact	Description of effect of hazard in the care setting and potential impact on the patient
Possible Causes	Possible cause(s) that may result in the hazard. These may be technical, human error, etc. Note: a hazard may have multiple causes
Existing Controls	Identification of existing controls or measures that are currently in place and will remain in place post implementation that provide mitigation against the hazard, i.e. used as part of initial Hazard Risk Assessment
Initial Hazard Risk Assessment	
• Severity	The severity of the hazard as defined in Table 7
• Likelihood	The likelihood of the hazard as defined in Table 8
• Risk Rating	The derived risk rating from the combination of likelihood and severity according to Table 9
Additional Controls	
• Design	Identification of design features or configurations implemented in the Health IT System in order to provide mitigation against the hazard.
• Test	Identification of testing to be completed in order to provide mitigation against the hazard
• Training	Identification of training to be implemented in order to provide mitigation against the hazard.
• Business Process Change	Identification of any Business Process Changes implemented in order to mitigate against the hazard
Residual Hazard Risk Assessment	
• Severity	The severity of the mitigated hazard as defined by Table 7
• Likelihood	The likelihood of the mitigated hazard as defined by Table 8
• Risk Rating	The derived mitigated risk rating from the combination of likelihood and severity according to Table 9
Actions	
• Summary	Summary of the action being taken with regard to mitigation of the hazard or individual causes
• Owner	The owner of the action
Hazard Status	The status of the hazard: • 'Open' not all clinical risk management actions, owned by the Manufacturer, in respect of this hazard, have been completed. • 'Transferred' all clinical risk management actions owned by the Manufacturer, in respect of this hazard, have been completed but not all actions, owned by the deploying Health Organisation, have been completed. • 'Closed' all clinical risk management actions in respect of this hazard have been completed.

Table 5 Hazard Log Entries

3.4 Clinical Safety Case

3.4.1	The Manufacturer MUST develop and maintain a Clinical Safety Case for the Health IT System.

The Clinical Safety Case is a structured argument which is supported by a body of relevant evidence that provides a compelling, comprehensible and valid case that a system is safe for release. The argument provides an explanation of how the supporting evidence can be interpreted as indicating that the Health IT System exhibits an adequate degree of safety, e.g. by demonstrating compliance with requirements or sufficient mitigation of identified hazards.

The supporting evidence is the result of observation, analysis, testing or simulation that provides information from which system safety can be claimed.

Parallels can be drawn between a Clinical Safety Case and legal proceedings:

- presentation of a defence (argument) without evidence is unfounded; how does the defence hold?
- presentation of evidence without a legal argument is unexplained; what is the meaning of the evidence?

The Clinical Safety Case should not be thought of as a physical issued document but rather the intellectual planning that needs to be considered and undertaken in order to establish the safety argument and generate the supporting evidence. Every effort should be made to establish the safety argument as soon as practical in the lifecycle. This will ensure that resource and effort is directed efficiently to generate relevant evidence. If consideration of the safety argument is left until later in the lifecycle it may become difficult to explain how the available evidence supports claims over the safety of the Health IT System. Such an approach may result in gaps or lack of evidence which may result in additional work, delays and increased costs.

The Clinical Safety Case will evolve during the lifecycle of the Health IT System and must be reviewed to ensure that it continues to provide sufficient confidence in the safety of the Health IT System.

The relationship between the Clinical Risk Management File, the Clinical Safety Case and the Clinical Safety Case Report can be understood by considering a filing cabinet:

- the filing cabinet itself can be thought of as the Clinical Risk Management File, i.e. the repository in which relevant information is stored
- the organisation, indexing and cross referencing of the information within the filing cabinet can be thought of as the Clinical Safety Case, i.e. the planning and structure

- the retrieval of information from the filing cabinet can be thought of as the Clinical Safety Case Report, i.e. presentation of information that has previously been organised to support a safety position at any point in time. It is permissible for this presentation to be incomplete at a particular point in time. For example, it may not be possible to present particular evidence at an early iteration of the report but it should to be possible to present the need for that evidence.

3.5 Clinical Safety Case Report

3.5.1	The Manufacturer MUST produce a Clinical Safety Case Report at each lifecycle phase defined in the Clinical Risk Management Plan.
3.5.2	A Clinical Safety Officer MUST approve each Clinical Safety Case Report.
3.5.3	The Manufacturer MUST make available each Clinical Safety Case Report to a receiving organisation, which may be a Health Organisation or another Manufacturer.

The Clinical Safety Case Report is the physical document that summarises all the key elements of the Clinical Safety Case and references all supporting material in a clear, comprehensible and concise format. It serves to communicate the Clinical Safety Case to the end users and Top Management but also where appropriate to other bodies such as regulators.

As the underlying Clinical Safety Case continues to evolve during the Health IT System lifecycle, then there is a need to issue Clinical Safety Case Reports in support of key milestones. The issuing of Clinical Safety Case Reports will be dictated by the Health IT System development lifecycle being followed as defined in the Clinical Risk Management Plan.

Typical development phases are detailed below. Generally, a Clinical Safety Case Report will be issued during but before completion of a phase. The principal motivation for issuing a Clinical Safety Case Report before completion of the phase is to support the decision to transition into the next development phase, e.g. via a design review and to influence, from a safety perspective the work conducted in the succeeding phase.

- Requirements Analysis: At this phase of the development the scope of the Clinical Safety Case Report will be limited to defining the scope of the Health IT System (4.2), identification of potential hazards (4.3) and estimation of the initial clinical risk (4.4). The purpose of issuing a Clinical Safety Case Report at this phase is to demonstrate that all perceivable hazards have been pre-empted and their clinical risk considered. The result of the clinical risk assessment establishes the safety requirements which are fed forward and addressed in the design phase.

- Design: At this phase of the development the scope of the Clinical Safety Case Report will extend to include the initial clinical risk evaluation (5.1) and where necessary clinical risk control option analysis (6.1). The purpose of issuing a Clinical Safety Case Report at this phase is to demonstrate that the clinical risk of the hazards identified during the requirements analysis phase has been evaluated and where necessary risk control methods have been identified and justified as being appropriate are addressed in the design. If the subsequent design activities establish new requirements then hazard identification (4.3) and risk estimation (4.4) activities need to be conducted. The Clinical Safety Case Report should present the residual clinical risk assuming successful implementation of the identified controls. Where the residual risk remains unacceptable, the Clinical Safety Case Report must present evidence to show that the manufacturer has undertaken a clinical risk benefits analysis (6.2).
- Test: At this phase of the development the scope of the Clinical Safety Case Report will extend to demonstrate implementation of the clinical risk control measures (6.3), where the owner of those controls is the Manufacturer. The purpose of issuing a Clinical Safety Case Report at this phase is to provide evidence that necessary risk control methods identified in the design phase have been implemented and the implementation is effective in reducing the clinical risk to the levels identified in the preceding Clinical Safety Case Report. If any defects are raised during testing then the clinical safety impact of any such defects needs to be considered and any identified risk managed in accordance with this standard.
- Delivery: At this phase of the development the scope of the Clinical Safety Case Report will extend to show completeness of clinical risk control (6.4). The purpose of issuing a Clinical Safety Case Report at this phase is to document completion of all the clinical risk management activities and to present the residual clinical risk at the point of the Health IT System being delivered by the Manufacturer for subsequent live use. Where any element of risk control is being transferred to a Health Organisation, for example the requirement to train end users, then this must be clearly communicated. The specific Health IT System release needs to be recorded.
- Modification: If during its lifetime, the Health IT System is modified, then the release of any such modification needs to be supported by a Clinical Safety Case Report. The Manufacturer will need to assess whether a single report can be issued at the delivery phase or whether reports will need to be issued at preceding phases as discussed above. The scale of change and its impact on clinical safety will dictate the approach taken. Again the Clinical Safety Case Report will need to specify the release highlighting the extent of the change introduced.

The specific time when a Clinical Safety Case Report is issued within a development programme will be influenced by many factors, including the development lifecycle that is being followed. It is important that the Manufacturer identifies these issue dates within the Clinical Risk Management Plan.

A single Clinical Safety Case Report may be maintained; being re-issued in accordance with local configuration control procedures, or individual standalone Clinical Safety Case Reports may be issued.

The Clinical Safety Case Report is the primary vehicle for presenting a statement of the clinical safety of the Health IT System. It therefore needs to be a readable document rather than simply a listing of the Clinical Safety Case or the content of the Clinical Risk Management File.

It needs to provide the reader with:

- a summary of all the relevant knowledge that has been acquired relating to the clinical risks associated with the Health IT System at that point in the lifecycle
- a clear and concise record of the process that has been applied to determine the clinical safety of the Health IT System
- a summary of the outcomes of the assessment procedures applied
- a clear listing of any residual clinical risks that have been identified and the related operational constraints and limitations that are applicable
- a clear listing of any hazards and associated clinical risks that have been transferred, together with any declared risk control measures, that are to be addressed as part of the Health Organisation clinical risk management process
- a listing of outstanding test issues / defects associated with the Health IT System which may have a clinical safety impact.

The structure of a Clinical Safety Case Report will reflect the organisation of the underlying Clinical Safety Case, which in turn will be influenced by the requirements of this standard. An example structure is provided in Table 6 but should not be considered to be prescriptive or definitive.

The Manufacturer's Clinical Safety Case Reports must be made available to the deploying Health Organisation. This deliverable is a key input into the Health Organisations clinical risk management activities in support of compliance with SCCI0160.

Where required and within the framework of any contract terms that exist between a Manufacturer and a Health Organisation, the Manufacturer needs to make available to the Health Organisation any documentation or evidence that is referenced within a Clinical Safety Case Report or which supports the underlying Clinical Safety Case.

It is strongly recommended that the Manufacturer proactively works in close collaboration with Health Organisations following delivery in order to ensure safe and effective deployment of the Health IT System. Such relationships will minimise the likelihood of unanticipated issues occurring and will ensure that any risk controls that the Manufacturer is dependent on the Health Organisation to implement are communicated across organisational boundaries.

1	**Introduction** Purpose of the Clinical Safety Case Report and phase of lifecycle it relates to.
2	**System Definition / Overview** Description of the Health IT System; identification of Health IT System part and version number; description of the clinical environment it is to be used in; description of any existing systems it replaces or interfaces with; number of users and patients.
3	**Clinical Risk Management System** Description of the Manufacturer's clinical risk management system; identification of key personnel, their roles and responsibilities; identification of clinical risk management governance structure.
4	**Clinical Risk Analysis** Hazard identification; description of patient safety consequences; explanation of hazard causes and contributory conditions; identification of existing mitigating controls; estimation of clinical risk; identification of participating personnel.
5	**Clinical Risk Evaluation** Evaluation of initial level of risk of each identified hazard using pre-defined criteria.
6	**Clinical Risk Control** Identification, justification, implementation and verification of adequate risk controls; residual clinical risk evaluation and completion of controls.
7	**Hazard Log** Presentation of associated Hazard Log.
8	**Test Issues** Summary of any outstanding test issues and the impact on clinical safety.
9	**Summary Safety Statement** Statement from the Clinical Safety Officer summarising the safety position of the Health IT System in the context of the intended deployment.
10	**Quality Assurance and Document Approval** Evidence of appropriate quality, review and approval regimes.
11	**Configuration Control / Management** Evidence of appropriate configuration control being used.

Table 6 Representative Content of a Clinical Safety Case Report

3.6 Safety Incident Management Log

3.6.1	The Manufacturer MUST maintain a Safety Incident Management Log.

The Manufacturer needs to establish and use a Safety Incident Management Log to support the effective communication, resolution and archiving of safety related incidents. The log should be used throughout the life of a Health IT System.

The Safety Incident Management Log should serve to provide a common portal to appropriate Manufacturer staff so that they have an up to date view of the status and management of both current and historical safety incidents associated with a Health IT System.

The requirement for a Safety Incident Log can be met through the use of an existing service management process but it will be necessary to identify those incidents that result or have the potential to result in a clinical risk.

The Safety Incident Management Log should record the following parameters:

- Reference Number: Unique identifier
- Reported by: Name and contact details of person reporting the incident
- Reported Date: Date on which the incident was reported
- Incident Summary: Narrative of incident including as much detail as is available including any prevailing conditions, causes and observed effects including any harm that occurred
- Clinical Risk Assessment: Determination of clinical risk by considering the severity of the incident, the likelihood of re-occurrence and known mitigation for relevant hazards
- System Release: Details of system affected
- Journal: Record of work conducted, including date and time, to resolve the incident. This entry would also identify any permanent risk control measures introduced to prevent re-occurrence. Should include “who” “when” and “what”
- Made Safe Date: Date at which the incident was made safe through the introduction of short-term risk controls
- Closed Date: Date at which the incident was resolved through the introduction of permanent risk control measures
- Cause: Summary of root cause analysis conducted.

4 Clinical risk analysis

4.1 Clinical risk analysis process

4.1.1	The Manufacturer MUST implement the clinical risk analysis activities defined in the Clinical Risk Management Plan.
4.1.2	Clinical risk analysis SHOULD be carried out by a multi-disciplinary group including a Clinical Safety Officer.
4.1.3	The extent of clinical risk analysis MUST be commensurate with the scale, complexity and level of clinical risk associated with the Release.

It is the responsibility of the Clinical Safety Officer to ensure that the clinical risk management activities are implemented as documented in the Clinical Risk Management Plan. Any departures from the Clinical Risk Management Plan should be documented within the Clinical Risk Management File. The Manufacturer may wish to update the Clinical Risk Management Plan in light of any such changes.

In order for the clinical risk analysis to be completed in a robust and competent manner it is essential that it is carried out by a group with representatives from all areas that are involved in the development and maintenance of the Health IT System. Clinicians that will use Health IT System after deployment should be included in the process. Involvement of a diverse set of expertise is more likely to result in hazards being identified which may have otherwise been missed.

Representatives from the following specialist areas will need to be involved in the clinical risk analysis, as appropriate:

- Clinical Safety Officer
- Subject Matter Experts / Specialists
- Message Analysts
- Technical Architects
- Clinical Users from the Health Organisation deploying the system
- Clinical Safety Officer from the Health Organisation deploying the system
- Programme Manager
- Quality Assurance
- Safety Engineering
- Risk Management
- Test Management and execution
- Quality Management.

4.2 Health IT System scope definition

4.2.1	The Manufacturer MUST define the clinical scope of the Health IT System which is to be delivered.
4.2.2	The Manufacturer MUST define the intended use of the Health IT System which is to be delivered.

Prior to commencing any hazard identification / risk assessment activity for a release it is essential to define the scope of the assessment. Defining the boundary correctly will limit the extent of the analysis as well as ensuring all areas impacted by the release are considered.

Clinical scope is the extent of the functionality that is provided within the Health IT System that can be used to support or influence the administration of healthcare to a patient.

Intended use is the definition or explanation of who will use the Health IT System and how they will use it, in terms of existing business processes or within new business process.

When defining the boundary of a clinical risk assessment the Manufacturer needs to consider the following where applicable:

- third party product integrated within the Health IT System to be released
- clinical process / use: understand the revised operations with the new solution and how the deploying Health IT System will impact on the current business processes and ways of working
- human interface: the interaction of users with the Health IT System and their behaviours using it
- IT Infrastructure: assess any infrastructure at the Health Organisation that is within the Manufacturer's scope of influence, required to support the deployment of the Health IT System. This may be achieved by the Manufacturer specifying the minimum system requirements
- data migration: where data migration is to be undertaken by the Manufacturer it should be included in the scope of the clinical risk management activities. Any hazards associated with the data migration should be analysed and suitably mitigated, working in conjunction with the relevant Health Organisation as appropriate.

4.3 Identification of hazards to patients

4.3.1	The Manufacturer MUST identify and document known and foreseeable hazards to patients with respect to the intended use of the Health IT System in both normal and fault conditions.

The Manufacturer will need to undertake and document hazard identification activities in order to reveal and document potential hazards to patients. Hazard identification needs to consider both normal and abnormal operating conditions and usage scenarios.

Many techniques exist for hazard identification and an appropriate technique will need to be chosen depending on the application and the available expertise. Example hazard identification techniques are presented in Appendix B.

In order to identify pertinent hazards the following three key areas must be considered:

- end to end clinical process, including functionality and how that functionality is used
- inter and intra Health IT System messaging
- Health IT System architecture and design.

It is strongly recommended that a hazard workshop is run to support complete hazard identification. Attendees at the workshop will be drawn from the areas identified in section 4.1 depending on the nature of the Health IT System.

The identified hazards and their causes shall be recorded in the Hazard Log. Examples of populated Hazard Logs are presented in Appendix A.

Details of the hazard workshop, including date, attendees and minutes should be recorded in the Clinical Risk Management File and documented in the Clinical Safety Case Report.

Where no clinical hazards are raised through the hazard identification activities then this judgement shall be recorded in the Clinical Risk Management File along with details of what was done, who carried out the assessment and the date of the assessment. As a result, the remaining clinical risk management activities defined in the clinical risk management process do not need to be conducted. Should any changes be proposed to the original scope or content of the Health IT System then the hazard identification shall be repeated to ensure that no hazards have been introduced as a result of the change. If this assessment identifies a new hazard then the clinical risk management process needs to be brought into play.

4.4 Estimation of the clinical risks

4.4.1	For each identified hazard the Manufacturer MUST estimate, using the criteria specified in the Clinical Risk Management Plan: • the severity of the hazard • the likelihood of the hazard • the resulting clinical risk.

The following classifications of likelihood, severity and resulting clinical risk are given for illustrative purposes only. It is for the Manufacturer to decide on the classifications to use for the release of a Health IT System. The assessment criteria which will be used shall be documented in the Clinical Risk Management Plan.

Further guidance on healthcare risk assessment has been published by the NPSA in their guide “Healthcare risk assessment made easy” [Ref. 9].

4.4.1 Assessment of Severity

The assessment of severity is made on a qualitative scale which should take account of the harm that might be experienced by patients if the hazard was to arise and an adverse event was to occur. The number of points on the qualitative scale for severity is a matter of choice by the Manufacturer. A five point scale might be:

- catastrophic
- major
- considerable
- significant
- minor.

Each severity category should have an associated meaning assigned. These meanings should be used to support the severity assessment made for each hazard. The provision of meanings will allow consistency of applications across hazards.

An illustration of a possible severity classification scheme is given in Table 7.

Severity Classification	Interpretation	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 severity	Single

Table 7 Example Severity Classification

This classification deals not only with physical injury but also with psychological trauma. It also distinguishes between harm to single and to multiple patients.

4.4.2 Assessment of Likelihood

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 judgement on a qualitative scale.

Where the likelihood of the identified hazard 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.

An example five point scale for likelihood is:

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

Each likelihood category should have an associated meaning assigned. These meanings should be used to support the likelihood assessment made for each hazard within the Clinical Safety Case Report. The provision of meanings, see Table 8, will allow consistency of applications across hazards

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

Table 8 Example Likelihood Classification

For each hazard the severity and likelihood assessment together with the resulting clinical risk shall be recorded in the Hazard Log. Any information required to support the assessment should be also be recorded in the Hazard Log.

4.4.3 Assessment of Risk

Clinical risk is defined as the combination of the severity of harm to a patient and the likelihood of occurrence of that harm. A two-dimensional clinical risk matrix, Table 9, is used to combine hazard likelihood and severity to yield a measure of risk.

Likelihood						
	Very High	3	4	4	5	5
	High	2	3	3	4	5
	Medium	2	2	3	3	4
	Low	1	2	2	3	4
	Very Low	1	1	2	2	3
		Minor	Significant	Considerable	Major	Catastrophic
		Severity				

Table 9 Example Clinical Risk Matrix

Controls that are in place prior to the deployment of the Health IT System and will still remain in place post deployment should be factored into the assessment.

The assessment of the hazard should consider the most realistic and typical scenario that could result in patient harm. It is possible that a hazard consequence may have more than one credible severity rating. For example the consequence of a patient being inadvertently prescribed an overdose of one particular drug could be more severe and immediate, giving little or no time for intervention, than the overdose of a different drug which may simply induce inconvenience after an elapsed period of time. The likelihood of the former occurring may be significantly lower than the latter if it is used to treat a very rare condition. The assessment needs to consider all scenarios and establish which is most credible.

It should be noted that a single hazard may have multiple possible causes. Where there are multiple possible causes the hazard risk assessment should be reported at the hazard level. In deriving the overall risk for a particular hazard, it is permissible to complete the Severity, Likelihood and Risk Rating cells for each individual cause. In this situation the most pessimistic Risk Rating for the related causes may be selected for the hazard.

5 Clinical risk evaluation

5.1 Initial clinical risk evaluation

5.1.1	For each identified hazard, the Manufacturer MUST evaluate whether the initial clinical risk is acceptable. This evaluation MUST use the risk acceptability criteria defined in the Clinical Risk Management Plan.
5.1.2	If the initial clinical risk is acceptable, then the risk control requirements defined in sections 6.1 to 6.3 do not apply to this hazard.

A key element of the clinical risk evaluation process is to gain:

- an understanding of the specific risk levels
- an understanding of where significant risks lie that may or may not subsequently be found capable of risk reduction to acceptable levels.

In order to establish risk acceptability, each clinical risk rating obtained from the risk matrix has to be compared against the risk acceptability criteria defined in the Clinical Risk Management Plan.

Controls that are in place prior to the deployment of the Health IT System and will remain in place post deployment should be factored into the assessment.

Definition of acceptable clinical risk is a decision for the Manufacturer, taking into account, as far as practical, the current values of society perhaps expressed in local, national or regional regulations. However, the general acceptability of an estimated risk, as defined in the risk matrix, (Table 9), is shown in Table 10.

5	Unacceptable level of risk
4	Mandatory elimination of hazard or addition of control measure to reduce risk to an acceptable level
3	Undesirable level of risk Attempts should be made to eliminate the hazard or implement control measures to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical
2	Acceptable where cost of further reduction outweighs benefits gained or where further risk reduction is impractical
1	Acceptable, no further action required

Table 10 Example Risk Acceptability Definitions

Risk control options will need to be identified for those risks that are considered unacceptable or undesirable, see section 6.

The results of the clinical risk evaluation and the rationale on which it is based are to be recorded in the Clinical Risk Management File.

6 Clinical risk control

6.1 Clinical risk control option analysis

6.1.1	The Manufacturer MUST identify appropriate clinical risk control measures to remove any unacceptable clinical risk.
6.1.2	Proposed clinical risk control measures MUST be assessed by the Manufacturer to determine whether: • new hazards will be introduced as a result of the measures • the clinical risks for previously identified hazards will be affected.
6.1.3	The Manufacturer MUST manage any new hazards or increased clinical risks in accordance with sections 4.4 to 6.4.
6.1.4	The Manufacturer MUST evaluate the residual clinical risk. This evaluation MUST use the risk acceptability criteria defined in the Clinical Risk Management Plan.
6.1.5	Where a residual clinical risk is judged unacceptable, the Manufacturer MUST identify additional clinical risk control measures in order to reduce the clinical risk.
6.1.6	If the Manufacturer determines that no suitable risk control measures are possible then the Manufacturer MUST conduct a clinical risk benefit analysis of the clinical risk (section 6.2).

Risk control options are to be investigated for each risk that has been evaluated as unacceptable. Whilst risk reduction might not be practicable in all cases, it should be considered.

Risk control measures can reduce the likelihood of the hazard occurring or reducing the severity if the hazard arises. For example, patient safety risks associated with provision of unintended medications may be reduced by using TallMan lettering to reduce the likelihood of errors being made in drug name perception or using native dm+d (dictionary of medicines and devices) terms to prevent communication errors between systems.

A reduction in risk can be achieved through the application of one or more of the following mechanisms, listed in order of preference:

- changes to the design or the inclusion of protective measures in the Health IT System
- product verification and validation (for example, testing). A testing programme should address each of the hazards and thus provide a practicable demonstration that the claimed risk reduction has been achieved
- administrative and implementation procedures
- user, operator and other stakeholder training and briefing
- information for patient safety, including warnings.

Where a Manufacturer is unable to implement a suitable clinical risk control measure, e.g. training required by Health Organisation staff, then the Manufacturer will ensure this need is clearly documented and communicated to the Health Organisation.

Once the risk control options have been identified the residual clinical risk needs to be evaluated using the criteria defined in the Clinical Risk Management Plan.

For each hazard, there are two possible results:

- the residual clinical risk is acceptable
- the residual clinical risk is unacceptable.

There is an important distinction to be made between residual clinical risks that are so low that there is no need to consider them and residual clinical risks that are greater than that but which are accepted because of the associated benefits and the impracticability of reducing the risks. If the residual clinical risk meets the Manufacturer's risk acceptability criteria then no further risk reduction is necessary.

An impact assessment of a proposed risk control measure should also be undertaken to determine if the risk control measure:

- creates a new hazard
- increases the estimated risk associated with another identified hazard.

Where this is the case, then the suitability of the proposed risk control measure should be re-evaluated. If no other option is available, then the new hazards or changed risks will themselves need to be managed in accordance with the risk management process.

The clinical risk control measures selected will need to be recorded in the Clinical Risk Management File.

6.2 Clinical risk benefit analysis

6.2.1	Where a residual clinical risk is deemed unacceptable and further clinical risk control is not practicable, the Manufacturer MUST determine if the clinical benefits of the intended use outweigh the residual clinical risk.
6.2.2	If the clinical benefits do not outweigh the residual clinical risk, then the clinical risk remains unacceptable and the project SHOULD be re-appraised.

Clinical risk benefit analysis is not required for every hazard.

Clinical risk benefit analysis is used to justify the residual clinical risk associated with a hazard 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 IT System is likely to provide more clinical benefit than harm.

The decision as to whether the residual clinical risk associated with a hazard is outweighed by the benefit the Health IT System provides is essentially a matter of judgement by experienced and knowledgeable individuals, which would normally include the Clinical Safety Officer. Unfortunately, there can be no standardised approach to estimate clinical benefit and a greater degree of variation will be the inevitable result of using different approaches.

Those involved in making clinical risk benefit judgements have a responsibility to understand and take into account the technical, clinical, regulatory, economic, sociological and political context of their risk management decisions.

If the analysis does not support the conclusion that the clinical benefits outweigh the residual clinical risk, then the clinical risk remains unacceptable.

However, the Health Organisation may be able to put in place additional control measures to those identified by the Manufacturer to further reduce the residual clinical risk. These additional external risk controls may then result in the acceptability criteria for a specific deployment being met. In such circumstances the Manufacturer needs to make sure that the Health Organisation understands that they are accepting certain residual risks that may arise in the use of the Health IT System. In such circumstances, the Health Organisation may decide that the clinical benefits outweigh the risk and the Health IT System can be delivered and deployed.

Generally, if all practicable clinical risk control measures, including those of an external Health Organisation are insufficient to satisfy the Manufacturer's clinical risk acceptability criteria, then the Health IT System should not be delivered. This decision should be communicated to the deploying Health Organisation.

It is possible (probable) that the risk acceptance criteria for a Manufacturer and a Health Organisation will be different. Inevitably some alignment will be required when assessing risk acceptability across organisational boundaries.

The clinical risk benefit analysis needs to be documented in the Clinical Safety Case Report and whether the residual clinical risk is now acceptable needs to be documented.

6.2.1 ALARP

The concept of ALARP (As Low As Reasonably Practicable) [Ref. 7] may be used to establish risk acceptance and justify the residual clinical risk associated with any identified hazard. Practicable has two elements:

- technical practicability; the ability to achieve further risk reduction
- economic practicability; the cost of achieving further risk reduction.

Any ALARP justification of residual clinical risk should consider these two elements.

Establishing whether a residual clinical risk is ALARP involves considering the level of risk remaining against the efforts required to reduce it further. The assessment is one of proportionality. Whilst it may be feasible to reduce the level of residual clinical risk through further mitigation or control the cost of doing so may be so great that it far outweighs the benefits to be gained in doing so. Conversely, there may be situations where for modest additional effort significant benefits in risk reduction could be realised.

ALARP is not prescriptive and requires expert judgement to be expressed in order to substantiate a claim of ALARP. Consequently any such assessment is always subjective. The ALARP triangle, shown in Figure C, depicts the concept.

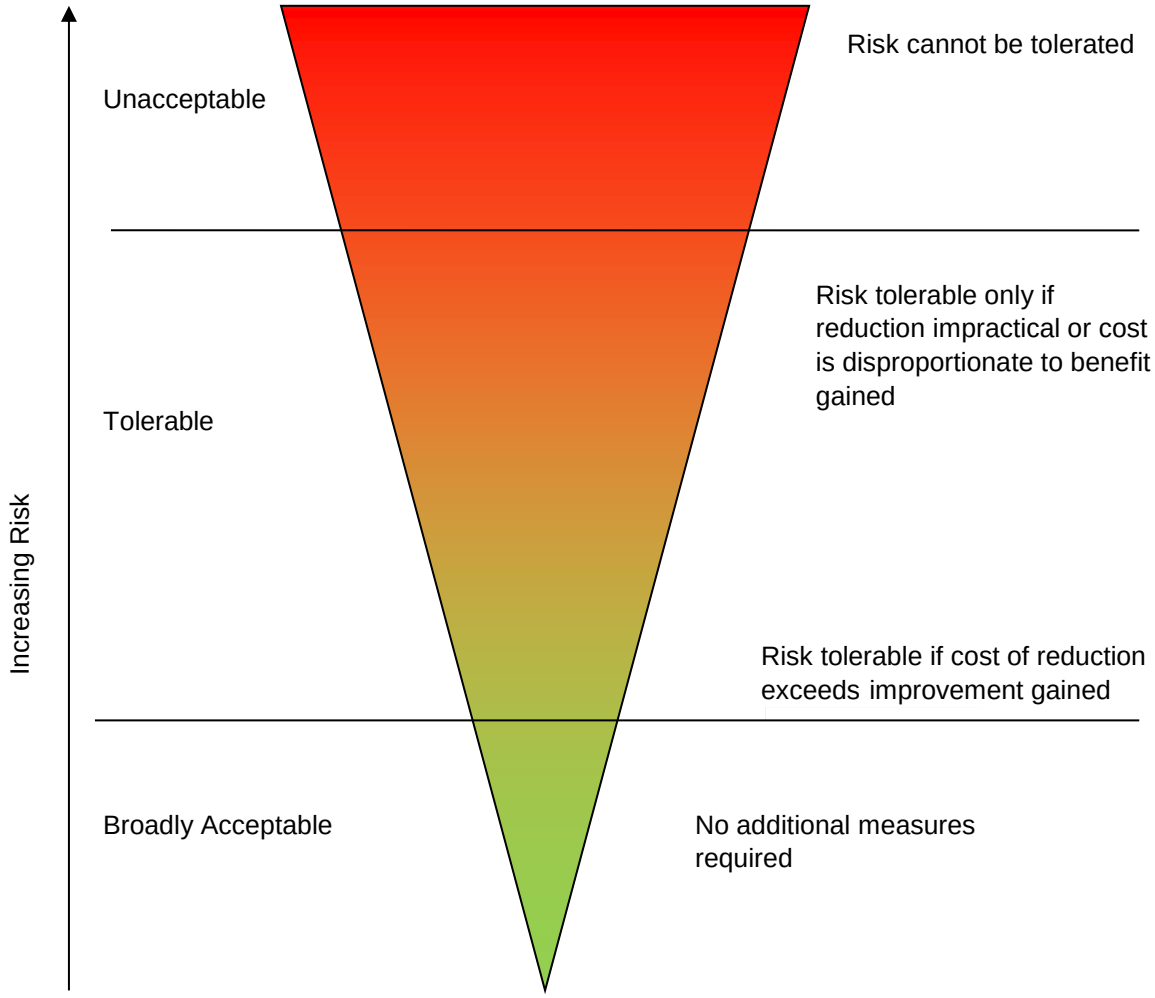

Figure C ALARP Triangle

6.3 Implementation of clinical risk control measures

6.3.1	The Manufacturer MUST implement the clinical risk control measures identified in section 6.1.1, except where these are to be implemented by another organisation.
6.3.2	The Manufacturer MUST verify each clinical risk control measure implemented under 6.3.1.
6.3.3	The Manufacturer MUST verify the effectiveness of each clinical risk control measure implemented under 6.3.1.

The Manufacturer must verify the implementation and effectiveness of the risk control measures for which they are responsible. Where a Manufacturer is dependent upon another organisation to implement further risk control measures in order to reduce the residual clinical risk to acceptable levels then they remain responsible for informing such organisations of their need to conduct the same activities.

Verification of a clinical risk control measure should consider both the implementation of the measure and the effectiveness of the measure.

The implementation verification activity, which should happen before delivery, is to confirm that the risk control measure is in place. The means and responsibility by which verification is carried out will depend on the nature of the measure.

Verifying the effectiveness of a clinical risk control measure demonstrates that the measure provides the intended result. Hence, effectiveness of a clinical risk control measure can only be determined with a clear understanding of the required effect of that clinical risk control measure.

The results of these activities will need to be recorded in the Clinical Safety Case Report.

6.4 Completeness of clinical risk control

6.4.1	The Manufacturer MUST ensure that the clinical risks from all identified hazards have been considered and accepted.

The Manufacturer of a Health IT System needs to be able to demonstrate that the clinical risk(s) from all identified hazards have been identified and considered and that the acceptability of all residual clinical risks is suitably justified.

Prior to delivery of any release a formal review will need to be conducted to ensure that the clinical risk management process as defined in the Clinical Risk Management Plan has been completed (see section 7.1).

The results of this review will need to be recorded in the Clinical Safety Case Report.

7 Delivery, Monitoring and Modification

7.1 Delivery

7.1.1	The Manufacturer MUST undertake a formal review of the Health IT System prior to its delivery to ensure that all of the requirements of this standard have been addressed.
7.1.2	The results of this review MUST be recorded in the Clinical Safety Case Report.
7.1.3	The Health IT System configuration for the release MUST be recorded in the Clinical Safety Case Report.

Prior to delivery of the Health IT System, the Manufacturer will need to undertake a formal review of the clinical risk management activities conducted to ensure that the requirements of this standard have been addressed.

The scale of this review should be commensurate with the scale of the overarching clinical risk management process but needs to be sufficient to ensure that Top Management are adequately appraised of the work conducted.

In essence the review needs to show that:

- the Manufacturer's Clinical Risk Management Plan has been implemented and the outcomes recorded
- the residual clinical risk for each hazard is acceptable
- appropriate methods are in place to obtain relevant post-deployment information and to feed these into the Manufacturer's clinical risk management system.

Top Management need to be satisfied that all foreseeable hazards have been identified and that the clinical risk of each hazard has been reduced to acceptable levels. In all circumstances, Top management remains responsible for the release of the Health IT System.

In addition, Top Management needs to be satisfied that any outstanding defects that remain unresolved at release have been reviewed by the Clinical Safety Officer and the potential impact on clinical safety has been assessed. If the risk of any such defects remains unacceptable then the Manufacturer must consider implementing additional risk control measures. Where further risk control measures are considered impractical then clinical risk benefits analysis needs to be conducted to establish whether the benefits of the release outweigh the residual clinical risk.

It may not be practical in all circumstances for a Manufacturer to implement adequate risk controls to reduce the risk to acceptable levels. In such circumstances a Manufacturer may identify the requirement for a Health Organisation to implement additional controls. Such requirements must be clearly documented in the Clinical Safety Case Report to ensure that a deploying Health Organisation is aware that an element of clinical risk is being transferred to it and that the Health Organisation will be responsible for implementing appropriate risk control measures.

This review and its findings must be recorded and summarised in the supporting Clinical Safety Case Report.

7.2 Post-deployment monitoring

7.2.1	The Manufacturer MUST establish, document and maintain a process to collect and review reported safety concerns and safety incidents for the Health IT System following its deployment.
7.2.2	The Manufacturer MUST assess the impact of any such information on the on-going validity of the Clinical Safety Case.
7.2.3	Where any such evidence is assessed to undermine the safety case the Manufacturer MUST take appropriate corrective action in accordance with the Clinical Risk Management Plan and document it in the Clinical Safety Case Report.
7.2.4	The Manufacturer MUST ensure safety related incidents are reported and resolved in a timely manner.
7.2.5	A record of safety incidents, including their resolution, MUST be maintained by the Manufacturer in a Safety Incident Management Log.

Once deployed, there is a need for the Manufacturer to proactively monitor and review the achieved safety characteristics of the Health IT System. This monitoring needs to extend beyond the Health IT System itself to include the impact on users and related healthcare processes.

The validity of any assumptions and the effectiveness of any controls made in the Clinical Safety Case Report need to be monitored to ensure the perceived level of clinical risk remains representative and acceptable. If it is found that the Clinical Safety Case does not hold in live system use, then the Manufacturer will need to undertake the clinical risk activities described in Sections 4 to 6 of the Standard. This may result in additional or modified clinical risk control mechanisms being introduced to manage the clinical risk. Any such changes need to be recorded in a re-issued Clinical Safety Case Report.

To support continued safe use of a Health IT System within a Health Organisation the Manufacturer needs to establish, implement and follow a safety incident management process.

The purpose of the safety incident management process is to:

- enable users of the Health IT System to report incidents, to the Manufacturer, they have had or they consider may have an impact on patient safety
- enable personnel within the Manufacturer’s organisation to report incidents they have had or they consider may have an impact on patient safety
- provide a communication mechanism within the Manufacturer’s organisation and where appropriate the Health Organisations that are using the Health IT System
- ensure appropriate and sufficient resources are allocated by the Manufacturer to manage and resolve the reported incident

- enable the Manufacturer to issue safety alerts or bulletins to Health Organisations to advise users of potential safety incidents and associated mitigation.

To achieve this, the safety incident management process needs to provide:

- a central point of contact (helpdesk) where the incident is logged
- a mechanism by which a clinical risk assessment can be made. In practice this will be the same criteria defined in the clinical risk management plan. As part of this assessment the existing safety case should be reviewed:
  - does the reported incident constitute a new hazard?
  - is the incident a realisation of a recorded hazard?
  - have clinical risk controls failed?
- a mechanism by which the user community can be advised of the safety incident
- a mechanism through which effective root cause analysis can be conducted. This mechanism will need to consider:
  - the provision of appropriate resource
  - collaboration with appropriate organisations
- corrective changes have been approved by the appropriate authority as identified in the Clinical Risk Management Plan
- appropriate key point indicators to ensure effective management
- a mechanism by which the user community can be advised that the safety incident has been resolved

If, as a consequence of an incident, the Clinical Safety Case is impacted then the Clinical Safety Case will need to be updated to capture this. In such circumstances the Manufacturer should consider issuing an updated Clinical Safety Case Report.

The reporting, management and resolution of each issue shall be recorded in a Safety Incident Management Log which will be referenced in the Clinical Risk Management File.

The requirement to record and manage safety incidents can be addressed by a Manufacturer in any existing service management framework, e.g. ITIL (IT Infrastructure Library), If this approach is followed then it will be necessary to be able to distinguish between those incidents that have a potential safety impact and any other incident recorded within that management system.

7.3 Modification

7.3.1	The Manufacturer MUST apply their clinical risk management process to any modifications or updates of the deployed Health IT System.
7.3.2	The application of this process MUST be commensurate with the scale and extent of the change and the introduction of any new clinical risks.

7.3.3	The Manufacturer MUST issue a Clinical Safety Case Report to support any modifications to the Health IT System that changes its clinical risk.
7.3.4	The Manufacturer MUST maintain an audit trail of all versions and patches released for deployment.

It is expected that a Health IT System will be modified or updated during its service. The motivation for any such changes could be defect fixes or introduction of new functionality. The Manufacturer will need to review its Clinical Safety Case to see if the modification or updates impact on existing hazards or introduces new hazards. In the event that the safety case is no longer valid the Manufacturer's Clinical Safety Case Report will need to be up-issued.

It is important that a direct correlation is maintained between a particular issue of a Clinical Safety Case Report and the corresponding Health IT System release. The Clinical Safety Case Report must record the specific Health IT System release it relates to. This record is in addition to any other configuration control processes used within a Manufacturer's organisation. This will need to be reviewed by the Health Organisation as part of their own clinical safety management activities to assess the impact on their own Clinical Safety Case.

The Manufacturer needs to create a log of all patches and modifications delivered into the NHS. This log should identify the release deployed at each Health Organisation. If an incident is reported which relates to a particular release of the Health IT System this information can be used to identify the extent of the issue and contact affected Health Organisations.

Appendix A Example Hazards

Two scenarios are presented below to illustrate example hazards, the potential safety consequence, the possible causes and associated controls(s) which all need to be considered when conducting the related risk assessment. It is important to record the correlation between the identified cause and associated control(s) so that the appropriateness and sufficiency of the control(s) can be evaluated. No risk assessment has been conducted and the associated columns have been omitted from the Hazard Log.

The key areas of Clinical Process (CP), Messaging (M) and Design (D) that are to be considered in hazard identification are also indicated in the examples.

A.1 Introduction of a new Patient Administration System into an acute hospital

This Hazard Assessment is set in the context of the introduction of a new Patient Administration System (PAS), replacing an existing manual administration and covers one particular scenario of a patient attending who is unable to provide their identity. It is assumed that existing manual processes will be retained to support the introduction of the new system to mitigate any inherent risk with the new system not being able to support care.

Hazard Number	Hazard Name	Hazard Description	Potential Clinical Impact	Possible Causes	Existing Controls	Additional Controls			
						Design	Test	Training	Business Process Change
1	Patient misidentification	Incorrect identification of presenting patient on their admission to hospital.	Presenting patient is incorrectly identified within the Patient Administration System and is mapped to another patient's medical record. Possibility that the patient subsequently receives inappropriate care or a delay in care.						
				Patient unknown to hospital and is unable to confirm their own identity (CP).	None, introduction of a new system	PAS design should support patient administration in emergency situations when their identity cannot be established.	PAS to be tested to assure correct implementation patient administration.	Hospital staff to be trained how to admit unidentified patients in emergency situations.	In emergency situations hospital procedures must allow temporary admission of patients even when their identity cannot be initially established.
				Patient's identity is similar to an existing patient held in PAS (CP).	None, introduction of a new system	PAS to implement NHS number	PAS to be tested to assure correct implementation of NHS number.	Hospital staff to be trained in use of NHS number as prime identifier.	Hospital procedures to accommodate use of NHS number as prime identifier.
				PAS human interface design is such that transcription or mis-selection errors occur; administrator believes that they have entered/selected correct demographic details for the presenting patient (D).	None, introduction of a new system	PAS to present demographic details in a format that clearly identifies differences. Design of PAS interface to comply with national standards	PAS interface design to be assessed by Manufacturer's CSO prior to release. PAS interface to be evaluated by hospital staff prior to release to ensure suitability.	Hospital staff trained to remain vigilant whilst identifying patient. Hospital staff trained in PAS use before deployment.	Hospital procedures to accommodate use of new PAS.

A.2 Introduction of a new electronic prescribing system in a GP surgery

This Hazard Assessment is focusing on the introduction of a new prescribing system and design and messaging flaws in that system that result in some error in the electronic prescription. There is an assumption that the dispensing system is working correctly and that existing competencies and procedures that already exist in the dispensing organisation would provide mitigation in the circumstance of the identified cause.

Hazard Number	Hazard Name	Hazard Description	Potential Clinical Impact	Possible Causes	Existing Controls	Additional Controls			
						Design	Test	Training	Business Process Change
2	Incorrect electronic prescription	Electronic prescription sent to dispensing pharmacy is different to what the prescriber intended.	On receipt at the dispensing pharmacy the electronic prescription contains different information to what the prescriber had intended or thought they had prescribed. Possibility that the patient receives the incorrect medications, dosage or quantity or suffers a delay in the administration of medications.						
				Faults in prescribing system that result in unintended but credible changes to the electronic message (D, M)	Existing dispensary competencies and procedures may alert dispenser to a problem and prevent unintended medications to be dispensed. In this case the patient would experience some delay. If prescriber suspects the system is not working correctly they can revert to paper prescribing.	Clinical safety design requirements to minimise likelihood.	Clinical safety testing by Manufacturer to assure system		

Hazard Number	Hazard Name	Hazard Description	Potential Clinical Impact	Possible Causes	Existing Controls	Additional Controls			
						Design	Test	Training	Business Process Change
				Incorrect mapping of medications within electronic prescribing system translates intended prescription into something different (D).	Existing dispensary competencies and procedures may alert dispenser to a problem and prevent unintended medications to be dispensed. In this case the patient would experience some delay. If prescriber suspects the system is not working correctly they can revert to paper prescribing.	Prescribing system to use native dm+d terms	Prescribing system to be tested to assure correct use of native dm+d	Surgery staff to remain vigilant whilst prescribing medication	
				Electronic prescription is routed to the incorrect dispensary (D, M)	No existing control to prevent immediate effect of patient experiencing a delay in the provision of their medication. If prescriber suspects the system is not working correctly they can revert to paper prescribing.	Clinical safety design requirements to minimise likelihood. Prescribing system to provide a prescription cancellation or recall capability.	Clinical safety testing by Manufacturer to assure system.		Surgery procedures to ensure an alternative prescription can be provided in such circumstances.

Appendix B Example Hazard Identification Techniques

B.1 FFA (Functional Failure Analysis)

B.1.1 Description

A hazard identification technique that takes a functional view of the system and for each function considers what the potential “safety consequences” may be if:

- the function is lost, i.e. not available when it is required
- the function is wrong, i.e. is available but performs an unintended action
- the function is provided when not required, i.e. function performs as intended but not at the correct time or out of sequence

Safety consequences document the potential consequence(s) the functional failure may have on a patient from which a hazard can be identified.

It considers “contributing factors” that may affect the safety outcome. Contributing factors include environmental conditions or other influences but excludes other functional causes within the system.

The analysis is captured and documented in a simple table.

B.1.2 Advantages

Simple analytical principles

Systematic and methodical technique which ensures all functionality is considered

Relatively efficient and can be conducted by a small team

Readily identifies those functions that are safety impacting.

B.1.3 Disadvantages

Can yield a massive amount of output if analysis is undertaken at too low a level of functional decomposition

Can be difficult to apply to systems where information is more important than function.

B.1.4 Example Analysis

This example considers the scenario where a Health IT System is being introduced into a social care organisation to provide Service Users with a facility to retrieve electronic demographic data. The availability or non-availability of paper based records within the social care organisation will have a direct impact on the safety consequences. Numbers are used to map the contributing causes with the respective safety consequence.

Function: Retrieve Personal Details		
Failure Mode	**Contributing Factors**	**Safety Consequences**
No Function: Service user demographics details are not available electronically to the Care Professional	1 No Paper records 2 Paper records are available and up to date. 3 Paper records are available but are out of date.	1 Delay in identifying Service User and completing contact assessment if demographic details are not available. Subsequent delay in assessing care needs and providing care services. Care services not provided. Hazard: Delay in provision of care services. Hazard: No provision of care services 2 Care professional would refer to paper records and conduct assessment on that basis. Little or no Service User harm 3 Care professional would refer to paper records but would conduct assessment on out of date data. Potential for provision of wrong or inappropriate care services. Hazard: Inappropriate care services provided.
Incorrect Function: Incorrect Service user demographic details presented electronically to the Care Professional	1 No Paper records. 2 Paper records are available and up to date. 3 Paper records are available but are out of date.	1 Care Professional conducts contact assessment using wrong demographic information. Subsequent care services could be based on another Service User's care history. Hazard: Inappropriate care services provided. 2 Care professional cross-checks with paper records (assumption). Little or no Service User harm

		3 Care professional cross-checks with paper records (assumption) and conducts contact assessment using out of date data. Potential for provision of wrong or inappropriate care services. Hazard: Inappropriate care services provided
Function Provided when not required	None	Distraction whilst using IT system No Service User harm - usability issue.

This table can be readily expanded to support hazard risk assessment.

Assessing the hazard “Delay in provision of care services” and considering the failure mode “No function” it’s reasonable to establish a cause as being a loss of connection to Spine within the system. The contributing factors can now be thought of as risk controls which in turn influence (in this example) the “Severity” assessment:

Function: Retrieve Personal Details						
Hazard	**Failure Mode**	**Cause**	**Existing Controls**	**Severity**	**Likelihood**	**Risk**
Delay in provision of care services	No Function: Service user demographics details are not available electronically to the Care Professional	No connection to Spine	None	Significant – delay in provision of care services could result in discomfort or short term harm. Not considered credible that care services would not be provided.	Medium – unproven new system	2 Acceptable where cost of further reduction outweighs benefits gained.
		No connection to Spine	Availability of paper records	Minor - Contact assessment can continue using existing paper based details (Assumption: paper records are maintained and up to date).	Medium – unproven new system	2 Acceptable where cost of further reduction outweighs benefits gained.
				Significant – severity of outcome increases in circumstances where paper records are not maintained. Delay in provision of care services could result in discomfort or short term harm. Not considered credible that care services would not be provided.	High – introduction of IT will reduce paper housekeeping	3 Undesirable Attempts should be made to eliminate the hazards or implement control measures to reduce risk to an acceptable level

B.2 HAZID (Hazard Identification)

B.2.1 Description

A hazard identification technique that focuses on the characteristics of information flow within a system. It is a structured brain storming technique which uses characteristic keywords (e.g. None, Wrong, Late, Incomplete Duplicate) to consider what the potential safety consequences may be. It can also be used to document the initial risk assessment.

The analysis is captured and documented in a simple table.

B.2.2 Advantages

Simple analytical principles

Systematic and methodical technique which ensures complete coverage

Readily identifies those functions that are safety impacting

Highly suited to IT systems where focus is the messaging and display of information.

B.2.3 Disadvantages

Can yield a massive amount of output if analysis is undertaken at too low a level of data definition

Generally requires a larger team and an experienced facilitator to keep task on track.

B.2.4 Example Analysis

This example considers the same scenario as B1 but the focus is the information (Demographic Details) rather than a particular function. Deviations in the intended characteristics of that data can then be considered to identify the potential safety consequences.

Contact Assessment					
Demographic Details (this is the information flow being analysed)					
Deviation Keyword	**Cause**	**Existing Controls**	**Consequences & Severity**	**Likelihood**	**Risk**
None					
Wrong					
Late					
Incomplete	Spine PDS record incomplete	Outside scope of Health IT System influence	N/A	N/A	N/A
	Incomplete record retrieved by Health IT System	Availability of paper based records to yield missing data	Minor - Missing information would be apparent and Contact Assessment can continue using paper based information.	Medium – unproven new system	2 Acceptable where cost of further reduction outweighs benefits gained.
Duplicate					

B.3 SWIFT (Structured What-IF Technique)

B.3.1 Description

A hazard identification technique that uses pertinent questions to explore the consequences of unintentional actions. It can include functions, information and users. It takes the form of a brain storming exercise with a strong cross section of relevant expertise.

The analysis is captured and documented in a simple table.

B.3.2 Advantages

Simple process that is easily followed.

Can identify significant issues quite quickly.

B.3.3 Disadvantages

Need relevant and appropriate set of questions if all issues are to be uncovered.

Can be difficult to do for the first time although generic themes (User Interface, Design Features, System Integration, Equipment Failures, Training) can be explored.

Can involve a large number of people.

Needs an experienced facilitator to ensure analysis stays focused.

B.3.4 Example Analysis

Task	Initial Contact Assessment					
Description of Task (input / output activity resource, equipment) Care Professional conducts contact assessment using local IT system to retrieve personal demographic details from NHS Spine to establish and confirm identity of Service User.						
What If Question	**Cause**	**Consequence**	**Safeguards**	**Current Risk**		
				S	**L**	**R**
Presenting Service User is unable to provide identity						
Care Professional is unable to enter right data						
IT system doesn't retrieve correct data from Spine						

B.4 Fishbone Diagram

B.4.1 Description

A root cause analysis technique which uses the concept of a fishbone to capture the causes to a pre-defined hazard.

A diagrammatical technique that enables the causes and the relationships between them to be conveyed.

B.4.2 Advantages

Intuitive technique that is easy to use and findings are readily conveyed

Generic themes can be used to prompt consideration of potential causes.

B.4.3 Disadvantages

Identification of hazard is a pre-requisite.

Limited expression of logical relationship between identified causes.

B.4.4 Example Analysis