England
(Link: /)

Digital

NHS Digital (Link: /)
Latest activity for information standards (Link: /data-and-information/information-standards/governance/latest-activity)
Standards and collections (Link: /data-and-information/information-standards/governance/latest-activity/standards-and-collections)
DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems

DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems

Prepared by the NHS Digital Clinical Safety team, this standard is designed to help health and care organisations assure the clinical safety of their health IT software

Review of digital clinical safety standards: DCB0129 and DCB0160

NHS England has started a review of digital clinical standards DCB0129 and DCB0160 (Link: /data-and-information/information-standards/governance/latest-activity/standards-and-collections/review-of-digital-clinical-safety-standards-dcb0129-and-dcb0160) to ensure they remain up-to-date, practical and aligned with the latest advancements in healthcare technology and clinical practice.

About this information standard

This standard provides a set of requirements suitably structured to promote and ensure the effective application of clinical risk management by those health organisations that are responsible for the deployment, use, maintenance or decommissioning of Health IT Systems within the health and care environment.

The standard includes implementation guidance and is supported by the related standard for the application of clinical risk management in the manufacture of Health IT Systems - DCB0129. (Link: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0129-clinical-risk-management-its-application-in-the-manufacture-of-health-it-systems)

This information standard is published under section 250 of the Health and Social Care Act 2012. An Information Standards Notice (see below) provides an overview of scope and implementation timescales, and the other documents provide further detail for those who have to implement the information standard.

October 2020: Update: Confirmation from the NHS Digital Clinical Safety Group that this has returned to business as usual activity.

Current release

Release date	07/06/2018
Release number	Amd 25/2018
Release title	2018 Update
Stage	Implementation
Key documents	• Change Specification (Amd 25/2018) (Link: /binaries/content/assets/website-assets/data-and-information/information-standards/standards-and-collections/dcb0160/0160252018changespec.pdf) • Specification (Amd 25/2018) (Link: /binaries/content/assets/website-assets/data-and-

information/information-standards/standards-and-collections/dcb0160/0160252018spec.pdf)

- Implementation Guidance (Amd 25/2018) (Link: /binaries/content/assets/website-assets/data-and-information/information-standards/standards-and-collections/dcb0160/0160252018impguid.pdf)
- Information Standards Notice (Amd 25/2018) (Link: /binaries/content/assets/website-assets/data-and-information/information-standards/standards-and-collections/dcb0160/0160382012isn.pdf)
- Guidance - determine the applicability of DCB 0129 and 0160 (Link: /services/clinical-safety/applicability-of-dcb-0129-and-dcb-0160)
- Compliance Assessment Template (Amd 38/2012) (Link: /binaries/content/assets/website-assets/data-and-information/information-standards/standards-and-collections/dcb0129-clinical-risk-management-its-application-in-the-manufacture-of-health-it-systems/dcb-0160-compliance-assessment-v5.0.xlsx)

Further information	Please see the NHS Digital website (Link: https://digital.nhs.uk/services/solution-assurance/the-clinical-safety-team) for further information about the Clinical Safety team.

Previous release

Release date	15/02/2013 (updated 05/05/2016)
Release number	Amd 38/2012
Release title	Version 3

Stage	Maintenance
Key documents	• Specification (Amd 38/2012) [Archive Content] (Link: /binaries/conten assets/data-and-information/information-standards/standards-collections/dcb0160/0160382012spec.pdf) • Implementation Guidance (Amd 38/2012) (Link: /binaries/content/ass assets/data-and-information/information-standards/standards-collections/dcb0160/0160382012imp-guide.pdf) • Information Standards Notice (Amd 38/2012) (Link: /binaries/content assets/isce/0160382012isn.pdf)
Guidance documents	• Agile Development (Amd 38/2012) (Link: /binaries/content/assets/w and-information/information-standards/standards-and-collections/dcb0160/0160382012agile.pdf) • Middleware (Amd 38/2012) (Link: /binaries/content/assets/website-information/information-standards/standards-and-collections/dcb0160/0160382012midd.pdf) • Telehealth and mobile health solutions (Amd 38/2012) (Link: /binaries/content/assets/website-assets/data-and-information/i standards/standards-and-collections/dcb0160/npfit-fnt-to-toclr 1311.02_crm_telehealth_development_implementation_guida
Previous releases	Please see the ISB website (Link: https://webarchive.nationalarchives.gov.uk/+/http:/www.isb.nhs.u for information on the previous releases.

Last edited: 15 June 2023 4:05 pm

Document filename: DCB0160 Change Specification v3.3.docx			
Directorate	Operations and Assurance Services	**Project**	Clinical Safety
Document Reference		**NPFIT-FNT-TO-TOCLNSA-1793.05**	
Director	Debbie Chinn	**Status**	Approved
Owner	Stuart Harrison	**Version**	3.3
Author	Sean White	**Version issue date**	11.05.2018

Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems – Change Specification

Copyright © 2018 NHS Digital

Document Management

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
	NHS Digital Clinical Safety Group	02.05.2018	3.3

Approved by

This document must be approved by the following people:

Name	Title	Date	Version
Dr Manpreet Pujara	Clinical Director for Patient Safety	02.05.2018	3.2
Debbie Chinn	Director of Solution Assurance	02.05.2018	3.2
	Publication Copy		3.2

Data Coordination Board

This information standard (DCB0160) has been approved for publication by the Department of Health and Social Care 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 Data Coordination Board (DCB), a sub-group of the Digital Delivery Board.

This information standard comprises the following documents:

- Requirements Specification
- Implementation Guidance
- Change Specification.

An Information Standards Notice (DCB0160 Amd 25/2018) 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 NHS Digital website. Any copies held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Date of publication: 7 June 2018

Copyright © 2018 NHS Digital

Contents

1 Purpose 4

2 Description 5

3 Future Consultation and Maintenance 6

Copyright © 2018 NHS Digital

1 Purpose

To inform those who have already implemented the standard what the changes are and how to implement those changes.

Copyright © 2018 NHS Digital

2 Description

This change focuses on aligning NHS Digital Clinical Safety standards with the new medical devices regulations for standalone software. The change provides clarity and removes uncertainty among users and developers with regard to the registration of software as a medical device and compliance with this standard. The evidence of this statement comes from academic and industry advisors, and recent experiences with devices in use that are decision making or supporting and integrated into unregulated software.

The new Medical Devices Regulation[1] was published by the European Commission in May 2017. A brief of it is:

- Software is specifically identified as a type of medical device. This will broaden the number of software solutions that are a medical device.
- Classification now includes risk as a component, in line with the NHS Digital Clinical Safety standards. This is important to note.
- The regulation includes additional essential requirements in the fields of:
    - IT environment
    - Interoperability
    - Cybersecurity
    - Mobile platforms
    - IT network and IT security.

This change in scope of the clinical risk management of health IT within the NHS Digital Clinical Safety standards provides a means of asserting compliance with this standard for the design, build, deployment and maintenance of software in conformance to a “harmonised” manner and in line with the medical devices regulations. A harmonised standard is a European standard developed by a recognised European Standards Organisation following a request from the European Commission.

Implementation Completion Date is 01/07/2018

[1] https://eur-lex.europa.eu/eli/reg/2017/745/oj

Copyright © 2018 NHS Digital

3 Future Consultation and Maintenance

In line with the approval by NHS Digital leadership teams to proceed with this change request and the endorsement of MHRA; the clinical safety team in NHS Digital are leading on the rewrite of ISO standards for clinical risk management of medical device software. The team will be monitoring implementation effectiveness within 6 months of publication and periodically as part of the quality function of this standard.

Copyright © 2018 NHS Digital

Document filename: DCB0160 Specification v3.2.docx			
Directorate	Operations and Assurance Services	**Project**	Clinical Safety
Document Reference		**NPFIT-FNT-TO-TOCLNSA-1793.05**	
Director	Debbie Chinn	**Status**	Approved
Owner	Stuart Harrison	**Version**	3.2
Author	Sean White	**Version issue date**	02.05.2018

Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems - Specification

Copyright © 2018 NHS Digital

Document Management

Revision History

Version	Date	Summary of Changes
0.1	06.10.2012	First draft for comment
0.2	22.10.2012	Revised following Information Standards Board appraisal
0.3	31.10.2012	Draft incorporating comments
0.4	11.12.2012	Draft incorporating comments identified in the review of ISB 1029
0.5	07.01.2013	For approval
0.6	09.01.2013	For review by Information Standards Management Service
0.7	17.01.2013	Review comments incorporated
1.0	21.01.2013	Approved
2.0	24.01.2013	Amended and Approved by ISMS Domain Leadership
3.0	08.12.2015	Amended and Approved to reflect change made to Requirement 2.6 (Non-health products and COTS is now Third party products)
3.1	16.08.2016	NHS Digital rebranded
3.2	02.05.2018	Changed to incorporate Medical Device Regulation and Data Coordination Board reference

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
	NHS Digital Clinical Safety Group	02.05.2018	3.2

Approved by

This document must be approved by the following people:

Name	Title	Date	Version
Dr Manpreet Pujara	Clinical Director for Patient Safety	02.05.2018	3.2
Debbie Chinn	Director of Solution Assurance	02.05.2018	3.2
	Publication Copy		3.2

Copyright © 2018 NHS Digital

Data Coordination Board

This information standard (DCB0160) has been approved for publication by the Department of Health and Social Care 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 Data Coordination Board (DCB), a sub-group of the Digital Delivery Board.

This information standard comprises the following documents:

- Requirements Specification
- Implementation Guidance
- Change Specification.

An Information Standards Notice (DCB0160 Amd 25/2018) 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 NHS Digital website. Any copies held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Date of publication: 7 June 2018

Copyright © 2018 NHS Digital

Related Documents:

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

Ref	Doc Reference Number	Title	Version
1.	DCB0160 Amd 25/2018	Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems: www.digital.nhs.uk/isce/publication/DCB0160	4.2
2.	DCB0129 Amd 24/2018	Clinical Risk Management: its Application in the Manufacture of Health IT Systems: www.digital.nhs.uk/isce/publication/DCB0129	3.2
3.	2017/745/EC	The EU Regulation on Medical Devices 2017/745	
4.	ISO 14971:2012	Medical Devices: Application of Risk Management to Medical Devices	2012
5.		ALARP (HSE Website)	
6.	0555	Healthcare risk assessment made easy, NPSA	2007
7.		Managing competence for safety-related systems, HSE	2007
8.	RFC-2119	Key words for use in RFCs to Indicate Requirement Levels, 1997	

Copyright © 2018 NHS Digital

Glossary of Terms:

Term	Definition
Clinical Safety Officer (previously referred to as Responsible Person)	Person in a Health 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 Health Organisation will conduct clinical risk management of a Health IT System.
Clinical risk management process	A set of interrelated or interacting activities, defined by the Health Organisation, to meet the requirements of this standard with the objective of ensuring clinical safety in respect to the deployment of a Health IT Systems.
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	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.

Copyright © 2018 NHS Digital

Initial clinical risk	The clinical risk derived during clinical risk estimation taking into consideration any retained risk control measures.
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 will include: 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) the Health Organisation and has overall accountability for a Health IT System.

Copyright © 2018 NHS Digital

Contents

1 Overview 9

1.1 Summary 9

2 General Requirements and Conformance Criteria for Clinical Risk Management 11

2.1 Clinical Risk Management Process 12
2.2 Top Management responsibilities 13
2.3 Clinical Safety Officer 13
2.4 Competencies of personnel 13
2.5 Intelligent procurement 13
2.6 Third party products 14
2.7 Regular clinical risk management process review 14

3 Project Safety Documentation and Repositories 15

3.1 Clinical Risk Management File 15
3.2 Clinical Risk Management Plan 15
3.3 Hazard Log 15
3.4 Clinical Safety Case 15
3.5 Clinical Safety Case Reports 16
3.6 Safety Incident Management Log 16

4 Clinical risk analysis 17

4.1 Clinical risk analysis process 17
4.2 Health IT System scope definition 17
4.3 Identification of hazards to patients 17
4.4 Estimation of the clinical risks 17

5 Clinical risk evaluation 18

5.1 Initial clinical risk evaluation 18

6 Clinical risk control 19

6.1 Clinical risk control option analysis 19
6.2 Clinical risk benefit analysis 19
6.3 Implementation of clinical risk control measures 20

Copyright © 2018 NHS Digital

6.4 Completeness of clinical risk control 20

7 Deployment, Maintenance and Decommission 21

7.1 Deployment 21
7.2 Post-deployment monitoring 21
7.3 Maintenance 21
7.4 Decommission 22

Copyright © 2018 NHS Digital

1 Overview

1.1 Summary

It is widely accepted that 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.

The use of such Health IT Systems is becoming increasingly widespread and the functionality is becoming more sophisticated. However, it must be recognised that failure, design flaws or incorrect use of such systems have the potential to cause harm to those patients that the system is intended to benefit.

The purpose of this standard is to promote and ensure that effective clinical risk management is carried out by those Health Organisations that are responsible for deploying, using, maintaining or decommissioning Health IT Systems within the NHS. This purpose is achieved through the presentation of a set of requirements.

Within this standard the term ‘clinical risk’ is used to emphasise that the scope is limited to the management of risks related to patient safety as distinct from other types of risk such as financial.

Clinical risk management may be conducted within the context of an overall risk management system operating within the Health Organisation and any wider health information governance processes. Wherever practical, existing risk management processes would be adapted and used to address the requirements of this standard.

The extent of clinical risk management needs only to be commensurate with the scale, complexity and level of clinical risk associated with the deployment. The Health Organisation’s clinical risk management processes should be flexible to facilitate this.

This standard is supported by implementation guidance [Ref. 1] which contains an explanatory narrative which will aid in the interpretation and application of this standard. This standard complements DCB0129 [Ref. 2].

This standard is addressed to those persons in Health Organisations who are responsible for ensuring clinical safety in the deployment of Health IT Systems through the application of clinical risk management.

For the purposes of this standard the terms ‘Clinician’ and ‘clinical’ includes all Health Organisations and personnel within the NHS who are deploying and using Health IT Systems. This standard applies to all Health IT Systems including those that are also controlled by medical device regulations [Ref. 3], though the requirements defined in this standard are broadly consistent with the requirements of ISO 14971 [Ref. 4].

Copyright © 2018 NHS Digital

Release	
Release Number	Amd 25/2018
Release Title	Version 3.2
Description	This change focusses on aligning NHS Digital Clinical Safety standards with the new medical devices regulations for stand alone software. The change provides clarity and removes uncertainty among users and developers with regard to the registration of software as a medical device and compliance with this standard. The evidence of this statement comes from academic and industry advisors, and recent experiences with devices in use that are decision making or supporting and integrated into unregulated software. The new Medical Devices Regulation was published by the European Commission in May 2017. A summary would include: • Software is specifically identified as a type of medical device. This will broaden the number of software solutions that are a medical device. • Classification now includes risk as a component, in line with the NHS Digital Clinical Safety standards. This is important to note. • The regulation includes additional essential requirements in the fields of: o IT environment o Interoperability o Cybersecurity o Mobile platforms o IT network and IT security. This change in scope of the clinical risk management of health IT within the NHS Digital Clinical Safety standards provides a means of asserting compliance with this standard for the design, build, deployment and maintenance of software in conformance to a “harmonised” manner and in line with the medical devices regulations. A harmonised standard is a European standard developed by a recognised European Standards Organisation following a request from the European Commission.
Implementation Completion Date	01.07.2018

Copyright © 2018 NHS Digital

2 General Requirements and Conformance Criteria for Clinical Risk Management

The following requirements use either MUST or SHOULD as defined in RFC-2119 [Ref. 8], where:

- MUST: “means that the definition is an absolute requirement of the specification”
- SHOULD: “means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course”.

In order to claim conformance with this Specification, a Health Organisation MUST implement the clinical risk analysis activities defined in sections 2 to 7, within the bounds of the definitions above.

Copyright © 2018 NHS Digital

2.1 Clinical Risk Management Process

2.1.1	The Health Organisation 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.*

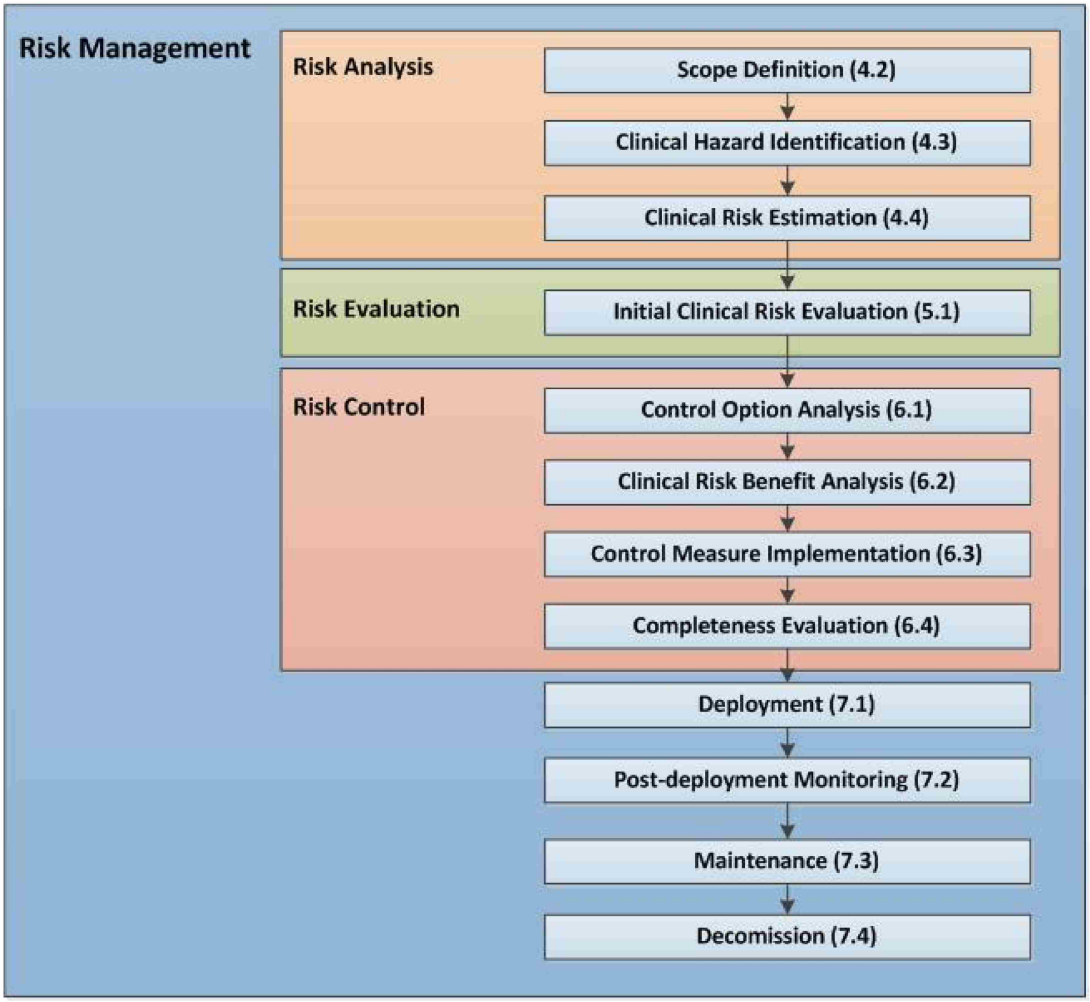


Figure 1 Clinical Risk Management Process

Copyright © 2018 NHS Digital

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 deploying and subsequently using the Health IT System • nominate a Clinical Safety Officer.
2.2.2	Top Management MUST authorise the deployment of the Health IT System accepting any residual clinical risk on behalf of the Health Organisation.

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.

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.

2.5 Intelligent procurement

2.5.1	In the procurement of a Health IT System the Health Organisation MUST ensure that the Manufacturer and the Health IT System complies with DCB0129. *Note: Under this requirement the Manufacturer will be required to make available applicable Clinical Safety Case Reports to aid the Health Organisation's own risk analysis.*

Copyright © 2018 NHS Digital

2.6 Third party products

2.6.1	The Health Organisation MUST assess any third party product used in a Health IT System as part of the clinical risk management process. *Note: Manufacturers who comply with DCB0129 are required to analyse any third party product which they incorporate into their Health IT System. The Manufacturer is also obliged to reveal what they have done in this context in Clinical Safety Case Reports.*

2.7 Regular clinical risk management process review

2.7.1	The Health Organisation MUST formally review its clinical risk management process at planned, regular intervals.

Copyright © 2018 NHS Digital

3 Project Safety Documentation and Repositories

This section defines the safety documents that are to be produced in support of the deployment of a Health IT System and mechanisms for their retention.

3.1 Clinical Risk Management File

3.1.1	The Health Organisation 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.

3.2 Clinical Risk Management Plan

3.2.1	The Health Organisation MUST produce at the start of a project a Clinical Risk Management Plan, which will include risk acceptability criteria, covering the deployment of a 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 deployment, use, maintenance or decommissioning 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.

3.3 Hazard Log

3.3.1	The Health Organisation 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.

3.4 Clinical Safety Case

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

Copyright © 2018 NHS Digital

3.5 Clinical Safety Case Reports

3.5.1	The Health Organisation MUST produce a Clinical Safety Case Report to support each lifecycle phase (i.e. deployment, use, maintenance and decommissioning) of the Health IT System.
3.5.2	A Clinical Safety Officer MUST approve each Clinical Safety Case Report.

3.6 Safety Incident Management Log

3.6.1	The Health Organisation MUST maintain a Safety Incident Management Log.

Copyright © 2018 NHS Digital

4 Clinical risk analysis

4.1 Clinical risk analysis process

4.1.1	The Health Organisation 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 deployment.

4.2 Health IT System scope definition

4.2.1	The Health Organisation MUST define the clinical scope of the Health IT System which is to be deployed.
4.2.2	The Health Organisation MUST define the intended use of the Health IT System which is to be deployed.
4.2.3	The Health Organisation MUST define the operational environment and users of the Health IT System which is to be deployed.

4.3 Identification of hazards to patients

4.3.1	The Health Organisation MUST identify and document known and foreseeable hazards to patients in both normal and fault conditions through the introduction and use of the Health IT System.

4.4 Estimation of the clinical risks

4.4.1	For each identified hazard the Health Organisation 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.

Copyright © 2018 NHS Digital

5 Clinical risk evaluation

5.1 Initial clinical risk evaluation

5.1.1	For each identified hazard, the Health Organisation 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.

Copyright © 2018 NHS Digital

6 Clinical risk control

6.1 Clinical risk control option analysis

6.1.1	The Health Organisation MUST identify appropriate clinical risk control measures to remove an unacceptable clinical risk.
6.1.2	Proposed clinical risk control measures MUST be assessed by the Health Organisation 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 Health Organisation MUST manage any new hazards or increased clinical risks in accordance with sections 4.4 to 6.4.
6.1.4	The Health Organisation 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 Health Organisation MUST identify additional clinical risk control measures in order to reduce the clinical risk.
6.1.6	If the Health Organisation determines that no suitable risk control measures are possible then the Health Organisation MUST conduct a clinical risk benefit analysis of the clinical risk (section 6.2).

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 Health Organisation 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 deployment SHOULD be re-appraised.

Copyright © 2018 NHS Digital

6.3 Implementation of clinical risk control measures

6.3.1	The Health Organisation MUST implement the clinical risk control measures identified in section 6.1.1.
6.3.2	The Health Organisation MUST verify each clinical risk control measure implemented under 6.3.1.
6.3.3	The Health Organisation MUST verify the effectiveness of each clinical risk control measure implemented under 6.3.1.

6.4 Completeness of clinical risk control

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

Copyright © 2018 NHS Digital

7 Deployment, Maintenance and Decommission

7.1 Deployment

7.1.1	The Health Organisation MUST assess any local customisations prior to deployment.
7.1.2	The Health Organisation MUST undertake a formal review of the Health IT System prior to its deployment to ensure that all of the requirements of this standard have been addressed.
7.1.3	The results of this review MUST be recorded in the Clinical Safety Case Report.

7.2 Post-deployment monitoring

7.2.1	The Health Organisation 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 Health Organisation 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 Clinical Safety Case, the Health Organisation 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 Health Organisation 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 Health Organisation in a Safety Incident Management Log.

7.3 Maintenance

7.3.1	The Health Organisation 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 Health Organisation MUST issue a Clinical Safety Case Report to support any modifications to the Health IT System that changes its clinical risk.

Copyright © 2018 NHS Digital

7.4 Decommission

7.4.1	The Health Organisation MUST apply their clinical risk management process to a Health IT System that is being decommissioned.
7.4.2	The application of this process MUST take into account the deployment of any succeeding Health IT System.
7.4.3	The application of this process MUST take into account the migration of data between the decommissioned Health IT System and the succeeding Health IT System.
7.4.4	The Health Organisation MUST issue a Clinical Safety Case Report to support decommissioning of the Health IT System.

Copyright © 2018 NHS Digital

Document filename: **DCB0160 Implementation Guidance v4.2.docx**			
Directorate	**Operations and Assurance Services**	Project	**Clinical Safety**
Document Reference		**NPFIT-FNT-TO-TOCLNSA-1293.06**	
Director	**Debbie Chinn**	Status	**Approved**
Owner	**Stuart Harrison**	Version	**4.2**
Author	**Sean White**	Version issue date	**02.05.2018**

Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems - Implementation Guidance

Copyright © 2018 NHS Digital

Document Management

Revision History

Version	Date	Summary of Changes
0.1	08.10.2012	First draft
0.2	15.10.2012	Second draft incorporating comments from National Integration Centre and Assurance Safety Engineers and Information Standards Board Appraisers
0.3	31.10.2012	Third draft incorporating review comments. Issued for approval
1.0	14.11.2012	Approved following incorporation of all comments
1.1	11.12.2012	Incorporation of changes following the appraisal of ISB 0129. Issued for approval
2.0	02.01.2013	Issued to Information Standards Management Services
2.1	17.01.2013	Incorporation of changes following review by Information Standards Management Services. For approval
3.0	21.01.2013	Approved
3.1	28.05.2013	HSCIC rebranded
4.0	08.12.2105	Amended and Approved to reflect change made to Requirement 2.6 (Non-health products and COTS is now Third party products)
4.1	16.08.2016	NHS Digital rebranded
4.2	02.05.2018	Changes to include Medical Device Regulation and Data Coordination Board reference

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
	NHS Digital Clinical Safety Group	02.05.2018	4.2

Approved by

This document must be approved by the following people:

Name	Title	Date	Version
Dr Manpreet Pujara	Clinical Director for Patient Safety	02.05.2018	4.2
Debbie Chinn	Director of Solution Assurance	02.05.2018	4.2
	Publication Copy		4.2

Copyright © 2018 NHS Digital

Data Coordination Board

This information standard (DCB0160) has been approved for publication by the Department of Health and Social Care 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 Data Coordination Board (DCB), a sub-group of the Digital Delivery Board.

This information standard comprises the following documents:

- Requirements Specification
- Implementation Guidance
- Change Specification.

An Information Standards Notice (DCB0160 Amd 25/2018) 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 NHS Digital website. Any copies held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Date of publication: 7 June 2018

Copyright © 2018 NHS Digital

Related Documents:

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

Ref	Doc Reference Number	Title	Version
1.	DCB0160 Amd 25/2018	Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems: www.digital.nhs.uk/isce/publication/DCB0160	3.2
2.	DCB0129 Amd 24/2018	Clinical Risk Management: its Application in the Manufacture of Health IT Systems: www.digital.nhs.uk/isce/publication/DCB0129	4.2
3.		ALARP (HSE Website)	
4.	0555	Healthcare risk assessment made easy, NPSA	2007
5.	2017/745/EC	The EU Regulation on Medical Devices 2017/745	
6.	ISO 14971:2012	Medical Devices: Application of Risk Management to Medical Devices	2012

Copyright © 2018 NHS Digital

Contents

1 Introduction 7

1.1 Background 7
1.2 Scope 7
1.3 Glossary of terms 8

2 General requirements for clinical risk management 10

2.1 Clinical risk management process 12
2.2 Top Management responsibilities 13
2.3 Clinical Safety Officer 15
2.4 Competencies of personnel 16
2.5 Intelligent procurement 17
2.6 Third party products 18
2.7 Regular clinical risk management process review 19

3 Project Safety Documentation and Repositories 20

3.1 Clinical Risk Management File 20
3.2 Clinical Risk Management Plan 20
3.3 Hazard Log 22
3.4 Clinical Safety Case 25
3.5 Clinical Safety Case Report 26
3.6 Safety Incident Management Log 29

4 Clinical risk analysis 30

4.1 Clinical risk analysis process 30
4.2 Health IT System scope definition 31
4.3 Identification of hazards to patients 32
4.4 Estimation of the clinical risks 33

5 Clinical risk evaluation 37

5.1 Initial clinical risk evaluation 37

6 Clinical risk control 38

6.1 Clinical risk control option analysis 38

Copyright © 2018 NHS Digital

6.2 Clinical risk benefit analysis 39
6.3 Implementation of clinical risk control measures 42
6.4 Completeness of clinical risk control 42

7 Deployment, Maintenance and Decommissioning 43

7.1 Deployment 43
7.2 Post-deployment monitoring 44
7.3 Maintenance 46
7.4 Decommission 47

Appendix A Example Hazards 48

A.1 Introduction of a new Patient Administration System into an acute hospital 48
A.2 Introduction of a new electronic prescribing system in a GP surgery 49

Appendix B Example Hazard Identification Techniques 51

B.1 FFA (Functional Failure Analysis) 51
B.2 HAZID (Hazard Identification) 55
B.3 SWIFT (Structured What-IF Technique) 57
B.4 Fishbone Diagram 59

Copyright © 2018 NHS Digital

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 has to be recognised that failure or incorrect use of such systems has the potential to cause harm to those patients that the system is intending to benefit.

This document provides guidance to support the interpretation of the requirements presented in DCB0160 [Ref. 1]. It is aimed at those persons in Health Organisations 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 Health 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 DCB0160 Specification [Ref. 1]. 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 deployment and use of a new Health IT System or in respect to the modification or decommissioning of an existing system. In this context modification may include changes to the Health IT System, the operational environment or clinical use.

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

Within this document the terms ‘Clinician’ and ‘clinical’ are used. For the purposes of this document these terms include all other healthcare organisations and personnel within the NHS who are deploying and using Health IT Systems.

In the deployment, use, modification or decommissioning 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

Copyright © 2018 NHS Digital

- environmental considerations
- organisational procedures.

This standard applies to all Health IT Systems including those that are also 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.

1.3 Glossary of terms

Term	Definition
Clinical Safety Officer (previously referred to as Responsible Person)	Person in a Health 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 Health Organisation will conduct clinical risk management of a Health IT System.
Clinical risk management process	A set of interrelated or interacting activities, defined by the Health Organisation, to meet the requirements of this standard with the objective of ensuring clinical safety in respect to the deployment of Health IT Systems.
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	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.

Copyright © 2018 NHS Digital

Term	Definition
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.
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 will include: 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) the Health Organisation and has overall accountability for a Health IT System.

Copyright © 2018 NHS Digital

2 General requirements for clinical risk management

In the deployment of a Health IT System, clinical risk management is an essential activity in ensuring the system does not compromise patient safety.

General requirements for effective clinical risk management are:

- a complete understanding of the Health IT System to be deployed and used
- 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 of any required clinical risk control measures
- any residual clinical risks are appropriately documented
- appropriate lifecycle management is in place.

Figure 1 presents a pictorial summary of the end-to-end clinical risk management process including the activities and documentation as required by the standard.

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.

Copyright © 2018 NHS Digital

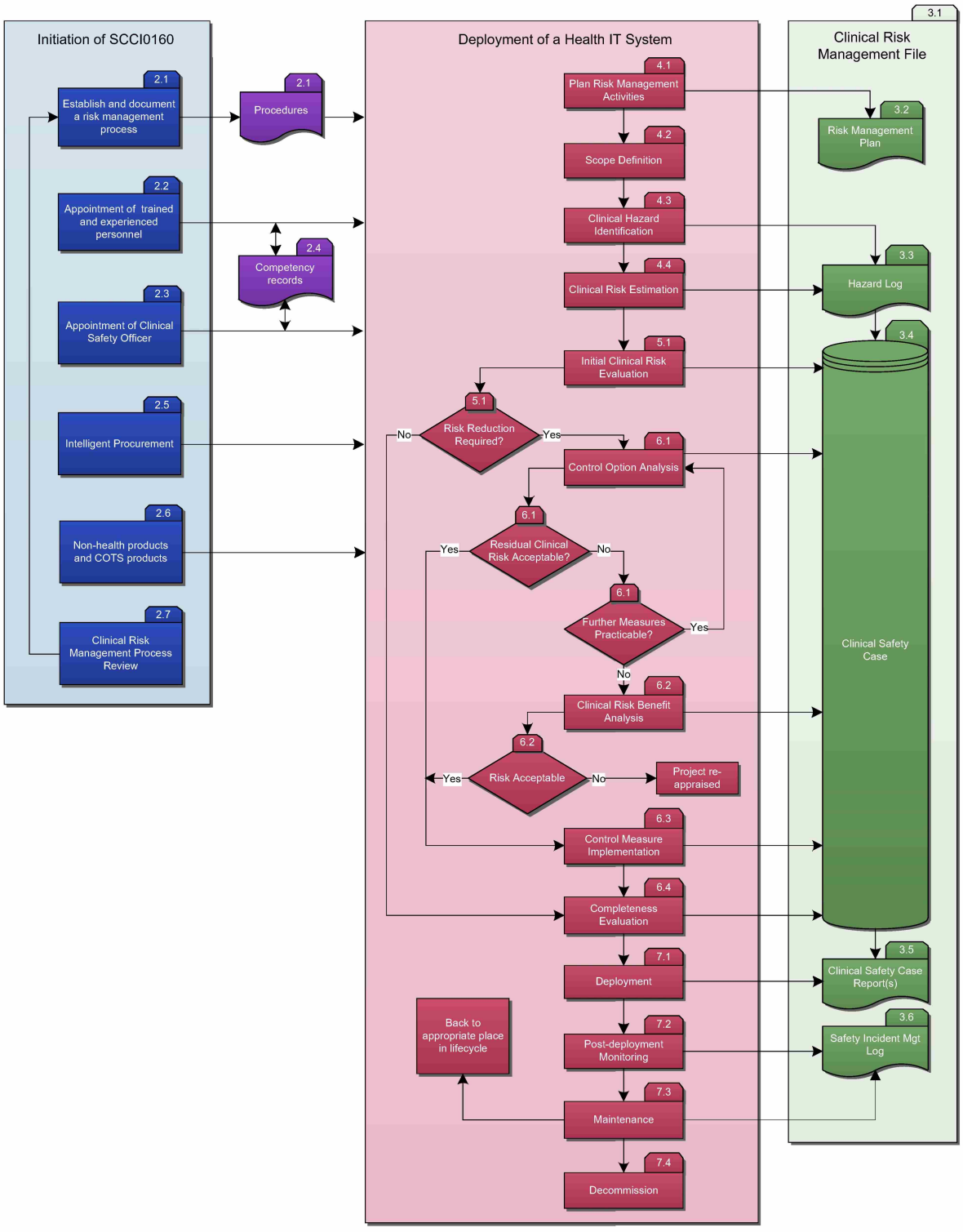


Figure 1 Clinical Risk Management Activities and Documentation

Copyright © 2018 NHS Digital

2.1 Clinical risk management process

2.1.1	The Health Organisation 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.*

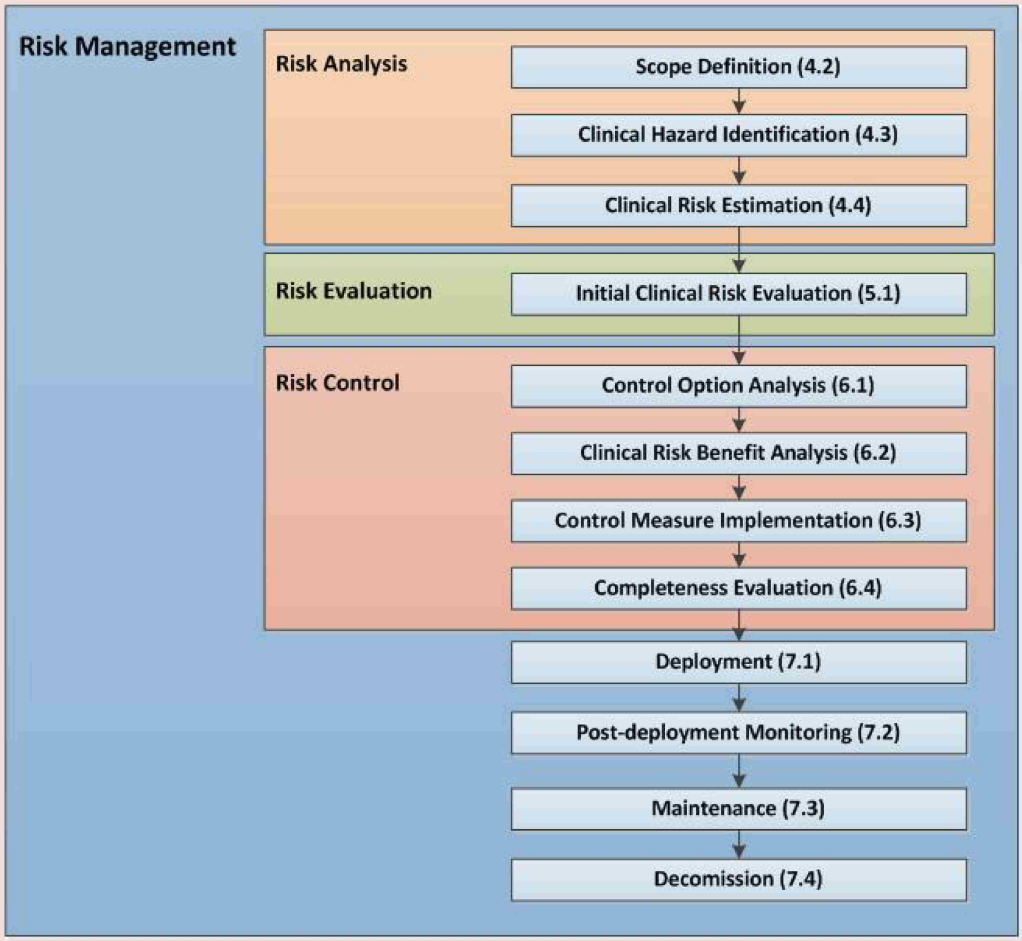


Figure 1 Clinical Risk Management Process

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

Copyright © 2018 NHS Digital

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 deployments; definitions of risk acceptability criteria, hazard severity and likelihood may vary across Health IT Systems. The Health Organisation is responsible for ensuring the clinical risk management process is applicable to a given deployment. Prior to tailoring the clinical risk management process, the Health Organisation will require a complete understanding of the system to be deployed and how it will be used.

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 deploying and subsequently using the Health IT System • nominate a Clinical Safety Officer.
2.2.2	Top Management MUST authorise the deployment of the Health IT System accepting any residual clinical risk on behalf of the Health Organisation.

Within the context of the standard, the interpretation of Top Management will differ across Health Organisations. As a guide, Top Management could be considered to be:

- Trust Board - Acute Trust
- Local Authority Director - Social Care
- Practice Manager - GP Surgery

It will be the responsibility of a Health Organisation to define its interpretation of Top Management as part of the clinical risk management process.

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 deployment.

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

Copyright © 2018 NHS Digital

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.

Representatives from each specialist area involved in deploying and subsequently using the Health IT System need to be appointed. 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. Typical specialist areas that may be required to support clinical risk activities are listed 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 is to be nominated for a given deployment. The Clinical Safety Officer will be responsible for ensuring the safety of a Health IT System in the Health Organisation 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 authorising the deployment of a Health IT System. 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 Health Organisation needs to undertake a formal review of the clinical risk management activities (see section 4.1) prior to the deployment 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 clinical risk of such hazards has been reduced to acceptable levels. By authorising the deployment of the Health IT System, Top Management is accepting any residual clinical risk on behalf of the Health Organisation.

Copyright © 2018 NHS Digital

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. 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 the key 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 deployment, modification and decommissioning
- 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 a recommendation to Top Management regarding whether the Health IT System is safe to deploy
- raise any unacceptable safety risks to Top Management.

Copyright © 2018 NHS Digital

COMPETENCY	RATIONALE
EXPERIENCE	
Relevant clinical experience	In depth knowledge 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 Health IT Systems, 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 reduce associated clinical risk.
SKILLS	
Critical appraisal and logical reasoning	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, able to identify root causes and propose practical and effective solutions from a clinical perspective.
Ability to facilitate consensus	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 Health Organisation 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 Health Organisation's competency framework.

Copyright © 2018 NHS Digital

Competency and experience records for personnel involved in the clinical risk activities need to be maintained in line with the Health Organisation'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.

2.5 Intelligent procurement

2.5.1	In the procurement of a Health IT System the Health Organisation MUST ensure that the Manufacturer and the Health IT System complies with DCB0129. *Note: Under this requirement the Manufacturer will be required to make available applicable Clinical Safety Case Reports to aid the Health Organisation's own risk analysis.*

Risks to patient safety can be considerably reduced through intelligent procurement. A formal framework for procurement should therefore be an integral component of clinical risk management. Examples would be the inclusion of safety impacting requirements in procurement contracts placed on the Manufacturer of the Health IT System.

The Health Organisation should:

- ensure that the Manufacturer has assessed the clinical risks associated with the Health IT System to be deployed in compliance with DCB0129 [Ref. 2]
- request that the Manufacturer's safety documentation is provided as this will form a key input into the Health Organisation's own clinical risk management activities
- request that a Manufacturer agrees to implement new or updated standards that are applicable to the Health IT System that is to be deployed.

The Health Organisation may procure and deploy a Health IT System from a Manufacturer which is not DCB0129 compliant. In this situation the Health IT System may not be supported by accompanying clinical risk management or safety documentation which may result in:

- an increased risk to patient safety
- the Health Organisation having to produce the safety material that should have been provided by the Manufacturer.

The Health Organisation, as a result of conducting its own clinical risk assessment, may decide that the benefits of deploying a Health IT System which does not satisfy the requirements of DCB0129 outweigh any associated risk to patient safety. The deployment of a non DCB0129 compliant Health IT System would have to be authorised by Top Management under requirement 2.2.2 of this standard.

Copyright © 2018 NHS Digital

As part of the procurement process the Health Organisation will need to review the list of standards and identify which are applicable to their deployment and ensure that the Health IT System is compliant with these standards. Such compliance could be achieved through inclusion in procurement contracts. Where a Health IT System is non-compliant a defensible reason for non-compliance has to be provided.

2.6 Third party products

2.6.1	The Health Organisation MUST assess any third party product used in a Health IT System as part of the clinical risk management process. *Note: Manufacturers who comply with DCB0129 are required to analyse any third party product which they incorporate into their Health IT System. The Manufacturer is also obliged to reveal what they have done in this context 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.

Where third party products and health software interact, the Health Organisation will need to ensure that its own clinical risk management process takes this into account.

Manufacturers who are compliant with DCB0129 are required as part of their clinical risk assessment activities to consider any third party product incorporated into their Health IT System. The Health Organisation should:

- confirm that any third party product used has been considered in the Manufacturer's safety documentation
- review the extent of the Manufacturer's contractual responsibilities for risk control both for original supply and for updates and patches which may be passed to the Health Organisation through them. In this situation there should be a requirement for the Manufacturer to maintain the associated Clinical Safety Case Report and provide updates highlighting changes in the level of risk.

Copyright © 2018 NHS Digital

2.7 Regular clinical risk management process review

2.7.1	The Health Organisation 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 deployments 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 Health Organisation in accordance with their management processes.

Copyright © 2018 NHS Digital

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 Health Organisation 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 guarantee that the Clinical Risk Management File and the artefacts it contains or references remain preserved and recoverable throughout the life of the Health IT System, including decommissioning.

3.2 Clinical Risk Management Plan

3.2.1	The Health Organisation MUST produce at the start of a project a Clinical Risk Management Plan, which will include risk acceptability criteria, covering the deployment of a 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 deployment, use, maintenance or decommissioning 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 deployment, maintenance and decommissioning of the Health IT System.

Copyright © 2018 NHS Digital

The Clinical Risk Management Plan should:

- define and describe the Health IT System and the clinical context in which it will be used
- state the relevant procedures, policies and resources required to ensure effective and efficient clinical risk management
- adhere to the Health Organisation's quality and project management processes and requirements
- define all the phases of the Health IT System lifecycle and quantify which clinical risk activities are applicable at a particular 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 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.

The extent of the Clinical Risk Management Plan needs to be commensurate with the scale and clinical functionality of the Health IT System 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 Health Organisation 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 deployment and use.

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

Copyright © 2018 NHS Digital

3.3 Hazard Log

3.3.1	The Health Organisation 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. 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.

Copyright © 2018 NHS Digital

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

Copyright © 2018 NHS Digital

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

Copyright © 2018 NHS Digital

3.4 Clinical Safety Case

3.4.1	The Health Organisation 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 a given application in a given operating environment. 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 is to 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

Copyright © 2018 NHS Digital

- 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 Health Organisation MUST produce a Clinical Safety Case Report to support each lifecycle phase (i.e. deployment, use, maintenance and decommissioning) of the Health IT System.
3.5.2	A Clinical Safety Officer MUST approve each Clinical Safety Case Report.

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.

Typically a Clinical Safety Case Report will be issued at:

- Pre Deployment: The Manufacturer's Clinical Safety Case Report will be a key input to support the transition to live use of the Health IT System. The scope of the Clinical Safety Case Report will extend to cover both normal and abnormal modes of system operation including associated recovery procedures. Human factors and the possibility of user error will be important considerations. Hazards identified in the Manufacturer's Clinical Safety Case Report and any assumptions made about clinical use will need to be considered in the specific deployment. The integration and the interaction of the Health IT System with other systems will also need to be considered from a clinical risk perspective.
- Post Deployment: If assumptions made at pre-deployment about the intended use or operating environment are not realised during use then the Clinical Safety Case will need to be re-examined and the effect on the Health IT System re-documented in a Clinical Safety Case Report. Similarly if the anticipated benefit of clinical risk control measures is not realised then the Clinical Safety Case will need to be re-examined and the effect on the Health IT System re-documented in a Clinical Safety Case Report

Copyright © 2018 NHS Digital

- Maintenance: If during use, the Health IT System is subjected to any change or modification or if its operating environment or clinical use is changed then the Clinical Safety Case Report needs to be re-evaluated and re-issued as appropriate. In practice this will involve undertaking clinical risk analysis, evaluation and control activities on the changes introduced and also on new or impacted interfaces within the system.
- Decommission: Here the focus of the clinical risk management process will be to identify, analyse, evaluate and control those hazards associated with removing the Health IT System from service rather than preserving the level of clinical risk associated with its use. Consideration needs to extend to include any clinical risk associated with retaining any clinical capability, existing interfaces with any other retained and integrated system, preservation and migration of health information and back-up or recovery requirements.

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.

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.

Copyright © 2018 NHS Digital

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 Health Organisation'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

Copyright © 2018 NHS Digital

3.6 Safety Incident Management Log

3.6.1	The Health Organisation MUST maintain a Safety Incident Management Log.

The Health Organisation 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 during the deployment, use, maintenance or decommissioning of a Health IT System. A Safety Incident Management Log could either be kept for a specific Health IT System or as a single central log.

The Safety Incident Management Log should serve to provide a common portal to all Health Organisation 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. Use of the log needs to be limited to record only 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, for example, prevailing conditions, causes and observed effects including any harm that occurred
- Clinical Risk Assessment: Determination of clinical risk by considering severity of the incident, the likelihood of re-occurrence and known mitigation for relevant hazards
- System Configuration: 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.

Copyright © 2018 NHS Digital

4 Clinical risk analysis

4.1 Clinical risk analysis process

4.1.1	The Health Organisation 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 deployment.

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 Health Organisation 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 deployment and subsequent use of the Health IT System. 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
- Clinical Users from each area affected by the deployment
- Internal IT department and other facilities management areas
- Other support departments, e.g. training, back office
- Programme Management
- Safety Engineering
- Risk Management
- Test Management and execution
- Clinical Governance
- Quality Management
- Business Change
- Manufacturer of Health IT System
- Manufacturer of interfacing systems / equipment.

Copyright © 2018 NHS Digital

4.2 Health IT System scope definition

4.2.1	The Health Organisation MUST define the clinical scope of the Health IT System which is to be deployed.
4.2.2	The Health Organisation MUST define the intended use of the Health IT System which is to be deployed.
4.2.3	The Health Organisation MUST define the operational environment and users of the Health IT System which is to be deployed.

Prior to commencing any hazard identification / risk assessment activity for a deployment 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 Health Organisation needs to consider the following:

- hazards identified in the Manufacturer's safety documentation and any associated clinical risk transferred to the Health Organisation
- 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
- interfaces: both internal and external interfaces between products should be a primary focus of the Health Organisation clinical risk assessment. It would be unreasonable to expect Manufacturers to have covered all possible linkages within their safety documentation as these are deployment specific. The interface should include messaging and transfer of data
- human interface: the interaction of users with the Health IT System and their behaviours using it
- IT Infrastructure: assessment as to whether the current IT infrastructure at the Health Organisation can support the deployment or whether there will be additional requirements for hardware, support etc.
- data migration: the Health Organisation should determine whether there is a requirement for data migration when an existing system is being replaced. Any hazards associated with the data migration process should be included in the clinical risk management activities
- local configuration: the Health Organisation should assess the potential impact of any local configuration changes as part of their risk management activities.

Copyright © 2018 NHS Digital

4.3 Identification of hazards to patients

4.3.1	The Health Organisation MUST identify and document known and foreseeable hazards to patients in both normal and fault conditions through the introduction and use of the Health IT System.

The Health Organisation 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 are to 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.

Copyright © 2018 NHS Digital

4.4 Estimation of the clinical risks

4.4.1	For each identified hazard the Health Organisation 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 Health Organisation to decide on the classifications to use for the deployment of a Health IT System. The assessment criteria to be used shall be documented in the Clinical Risk Management Plan.

Further guidance on healthcare risk assessment has been published by the National Patient Safety Agency (NPSA) in their guide "*Healthcare risk assessment made easy*" [Ref. 4].

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 the severity is a matter of choice by the Health Organisation. 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.

Copyright © 2018 NHS Digital

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.

Copyright © 2018 NHS Digital

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 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 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 risk assessment should consider all the hazard scenarios and establish the associated severity and likelihood ratings. Where the hazard cause is common in the different scenarios then the highest risk rating should be used. In practice, the Clinical Risk Matrix will ensure that extreme combinations of severity and likelihood yield the same or very similar risk rating.

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.

Copyright © 2018 NHS Digital

5 Clinical risk evaluation

5.1 Initial clinical risk evaluation

5.1.1	For each identified hazard, the Health Organisation 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 still remain in place post deployment should be factored into the assessment.

Definition of acceptable clinical risk is a decision for the Health Organisation, 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 hazards or addition of control measures to reduce risk to an acceptable level
3	Undesirable level of risk Attempts should be made to eliminate the hazards 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.

Copyright © 2018 NHS Digital

6 Clinical risk control

6.1 Clinical risk control option analysis

6.1.1	The Health Organisation MUST identify appropriate clinical risk control measures to remove an unacceptable clinical risk.
6.1.2	Proposed clinical risk control measures MUST be assessed by the Health Organisation 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 Health Organisation MUST manage any new hazards or increased clinical risks in accordance with sections 4.4 to 6.4.
6.1.4	The Health Organisation 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 Health Organisation MUST identify additional clinical risk control measures in order to reduce the clinical risk.
6.1.6	If the Health Organisation determines that no suitable risk control measures are possible then the Health Organisation MUST conduct a clinical risk benefit analysis of the clinical risk (section 6.2).

Risk control options are to be investigated for each clinical 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 lessen the severity if the hazard arises. For example, clinical risks resulting from a single point of failure on a network may be reduced by eliminating that single point of failure (for example, adding a redundant link) or by reducing effects of failure (for example, notification of the link being lost).

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.

Copyright © 2018 NHS Digital

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 Health Organisation'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 Health Organisation 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 deployment 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 risks associated with a hazard is outweighed by the benefits 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.

Copyright © 2018 NHS Digital

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. Generally, if all practicable clinical risk control measures are insufficient to satisfy the clinical risk acceptability criteria, then approval to deploy and use the system should not be granted.

Proceeding with a deployment that retains unacceptable risk would need explicit approval by Top Management using established governance processes. In such a case, the clinical risk would have to be communicated across the Health organisation to ensure full awareness.

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. 3] 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 2, depicts the concept.

Copyright © 2018 NHS Digital

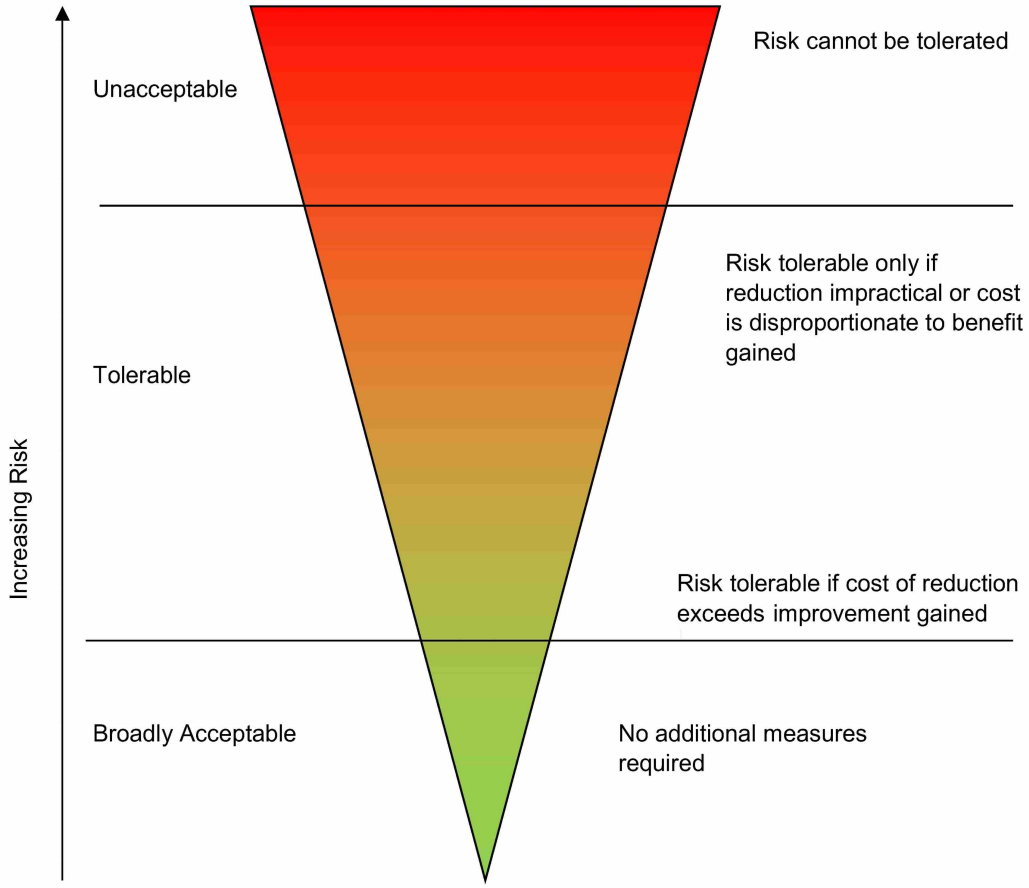


Figure 2 ALARP Triangle

Copyright © 2018 NHS Digital

6.3 Implementation of clinical risk control measures

6.3.1	The Health Organisation MUST implement the clinical risk control measures identified in section 6.1.1.
6.3.2	The Health Organisation MUST verify each clinical risk control measure implemented under 6.3.1.
6.3.3	The Health Organisation MUST verify the effectiveness of each clinical risk control measure implemented under 6.3.1.

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 go-live, is to confirm that the risk control measure has been enacted. 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. For example, a clinical risk control measure for network link failure can be the provision of a redundant link. Verification of effectiveness would involve simulating a primary link failure and verifying the redundant link was effective.

In some cases effectiveness cannot be verified objectively, for example, in the case of additional training, and changes to business processes and procedures. Here, additional monitoring is appropriate.

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 Health Organisation MUST ensure that the clinical risks from all identified hazards have been considered and accepted.

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

Prior to any deployment 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 3.2).

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

Copyright © 2018 NHS Digital

7 Deployment, Maintenance and Decommissioning

7.1 Deployment

7.1.1	The Health Organisation MUST assess any local customisations prior to deployment.
7.1.2	The Health Organisation MUST undertake a formal review of the Health IT System prior to its deployment to ensure that all of the requirements of this standard have been addressed.
7.1.3	The results of this review MUST be recorded in the Clinical Safety Case Report.

Prior to deployment of the Health IT System for live use, the Health Organisation 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 Health Organisation's Clinical Risk Management Plan has been implemented and the outcomes recorded
- the Clinical Safety Case Report supplied by the Health IT System Manufacturer has been reviewed in the context of the intended deployment
- the agreed controls have been implemented
- 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 Health Organisation's clinical risk management system and where appropriate to the Health IT System Manufacturer.

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 deployment of the Health IT System.

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

Copyright © 2018 NHS Digital

7.2 Post-deployment monitoring

7.2.1	The Health Organisation 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 Health Organisation 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 Health Organisation 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 Health Organisation 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 Health Organisation in a Safety Incident Management Log.

Once deployed, there is a need 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, related healthcare processes and any change in intended use.

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 Health Organisation 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 measures being introduced to manage the clinical risk. Any such changes need to be recorded in a re-issued Clinical Safety Case Report.

To support safe deployment and subsequent live use of a Health IT System it is imperative that the Health Organisation 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 they have had or they consider may have an impact on patient safety
- provide a communication mechanism within the Health Organisation and where appropriate the Manufacturer of the Health IT System
- ensure appropriate and sufficient resources are allocated by the Health Organisation to manage and resolve the reported incident
- enable the Health Organisation to respond to any safety alerts or bulletins issued by the Manufacturer of the Health IT System.

Copyright © 2018 NHS Digital

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 the Health IT System Manufacturer
  - collaboration with wider user community
- appropriate authorities to deploy system changes, make business process amendments and close the incident
- 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 Health Organisation 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.

Copyright © 2018 NHS Digital

7.3 Maintenance

7.3.1	The Health Organisation 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 Health Organisation MUST issue a Clinical Safety Case Report to support any modifications to the Health IT System that changes its clinical risk.

Many Health IT Systems can be configured or customised to support a particular local requirement. In such cases the Health Organisation needs to review the Manufacturer's Clinical Safety Case Report to be satisfied that it remains applicable in their own particular context. It is feasible that a Manufacturer may not have considered all possible configurations of their Health IT System within the scope of their clinical risk management activities. If any gaps are identified then sufficient clinical risk management needs to be conducted. In practice this could be done by the Manufacturer, Health Organisation or (preferably) jointly. The approach followed will largely be dictated by local contract arrangements.

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. A Health Organisation should expect their Health IT System Manufacturer to review its own safety case in support of any such change. 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 changes introduced also need to be individually assessed by the Health Organisation. Where it is established that the change or update impacts on existing hazards or introduces new hazards the Health Organisation's Clinical Safety Case Report will need to be up-issued.

Copyright © 2018 NHS Digital

7.4 Decommission

7.4.1	The Health Organisation MUST apply their clinical risk management process to a Health IT System that is being decommissioned.
7.4.2	The application of this process MUST take into account the deployment of any succeeding Health IT System.
7.4.3	The application of this process MUST take into account the migration of data between the decommissioned Health IT System and the succeeding Health IT System.
7.4.4	The Health Organisation MUST issue a Clinical Safety Case Report to support decommissioning of the Health IT System.

Health IT Systems that are being decommissioned from use will need to be subject to the same clinical risk management activities as when they were first deployed. At this point in the lifecycle the focus will be on controlling the risk of hazards associated with the removal of the Health IT System from service.

There is a need to consider potential hazards and associated risks related to:

- removing the health IT functionality from the Health Organisation and the impact this will have on healthcare provision
- introduction of new or amended business processes to compensate for the loss of the Health IT System
- an inability to retain and recover health information following decommissioning.

Where the decommissioned Health IT System is to be replaced or an alternative used then there is a need to consider potential hazards and associated risks related to:

- providing the health IT functionality in a successor or alternative Health IT System
- an inability to migrate health information into a successor or alternative Health IT System
- continuity of healthcare provision during the cut-over to a successor Health IT System
- changes to user's training requirements and needs.

At the point of decommission, the Health Organisation's Clinical Safety Case Report will need to be re-issued except where no clinical hazards are identified with respect to decommissioning the Health IT System. In this case 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.

Copyright © 2018 NHS Digital

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.

Copyright © 2018 NHS Digital

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		

Copyright © 2018 NHS Digital

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.

Copyright © 2018 NHS Digital

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.

Copyright © 2018 NHS Digital

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).

Copyright © 2018 NHS Digital

		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.

Copyright © 2018 NHS Digital

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

Copyright © 2018 NHS Digital

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.

Copyright © 2018 NHS Digital

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					

Copyright © 2018 NHS Digital

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.

Copyright © 2018 NHS Digital

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						

Copyright © 2018 NHS Digital

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.

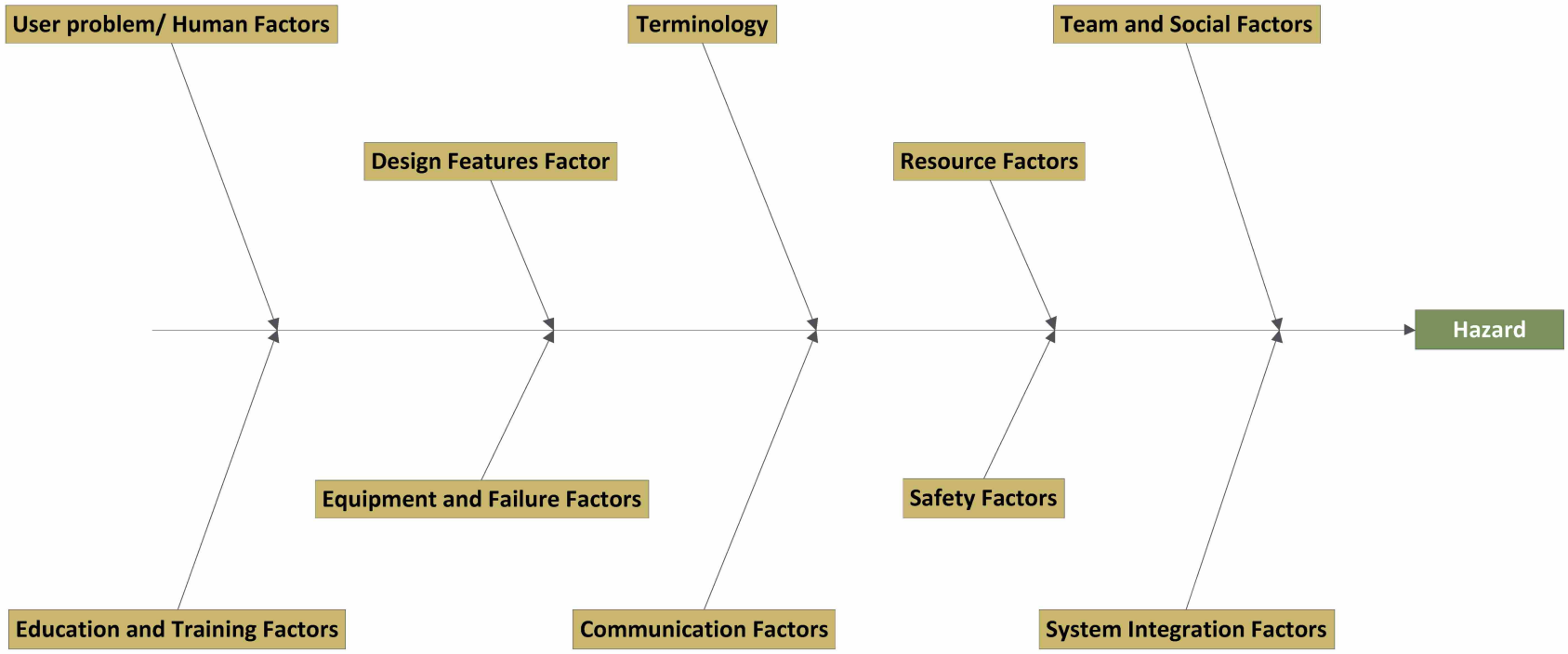
B.4.3 Disadvantages

Identification of hazard is a pre-requisite.

Limited expression of logical relationship between identified causes.

Copyright © 2018 NHS Digital

B.4.4 Example Analysis



Copyright © 2018 NHS Digital

Data Coordination Board

Information Standards Notice – Change

Acting under delegated authority from the Secretary of State for Health and Social Care, the Data Coordination Board (DCB) has approved a change to an existing information standard for publication under section 250 of the Health and Social Care Act 2012.

You must comply with the change to this standard by the full conformance date specified below.

Standard details	
DCB unique identifier	DCB0160 Amd 25/2018
Name	Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems, 2018 Update
Approval date	29 May 2018
Publication date	7 June 2018
Standard definition	
Description	This information standard provides a set of requirements suitably structured to promote and ensure the effective application of clinical risk management by health and care organisations deploying and using Health IT Systems. The standard forms part of the NHS Digital Clinical Safety Standards; it is accompanied by the related standard for the application of clinical risk management in the manufacture of Health IT Systems (DCB0129).
About this change	Following the publication of the Medical Devices Regulation (EU 2017/745) in May 2017 and evidence of the need for clinical risk assessment of medical devices using software, a decision has been made to extend the scope of the standard to now include medical devices. Previously medical devices have been excluded from the scope of the Clinical Safety Standards.
Scope (Health and Social Care Act 2012)	Health Services, NHS Services, Adult Social Care
Applies to	This information standard is addressed to health organisations that are responsible for ensuring clinical safety in the deployment, use, maintenance or decommissioning of Health IT Systems through the application of clinical risk management.
Legal authority	This information standard is published under section 250 of the Health and Social Care Act 2012.
Link to further documentation	The Change Specification, Requirements Specification and Implementation Guidance are available on the NHS Digital website: www.digital.nhs.uk/isce/publication/dcb0160

Data Coordination Board

Contacts	
Sponsor	Manpreet Pujara, Clinical Director for Patient Safety, NHS Digital
SRO	Stuart Harrison, Head of Safety Engineering, NHS Digital
Business Lead	Sean White, Principal Practitioner Solution Assurance, NHS Digital
Help Desk	enquiries@nhsdigital.nhs.uk
Dates	
Implementation completion date	1 July 2018
Post Implementation Review date	31 December 2018

The controlled version of this Information Standards Notice is published on the NHS Digital website: http://www.digital.nhs.uk/isce/publication/isns