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.

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

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].

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: ○ 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	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.

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.*

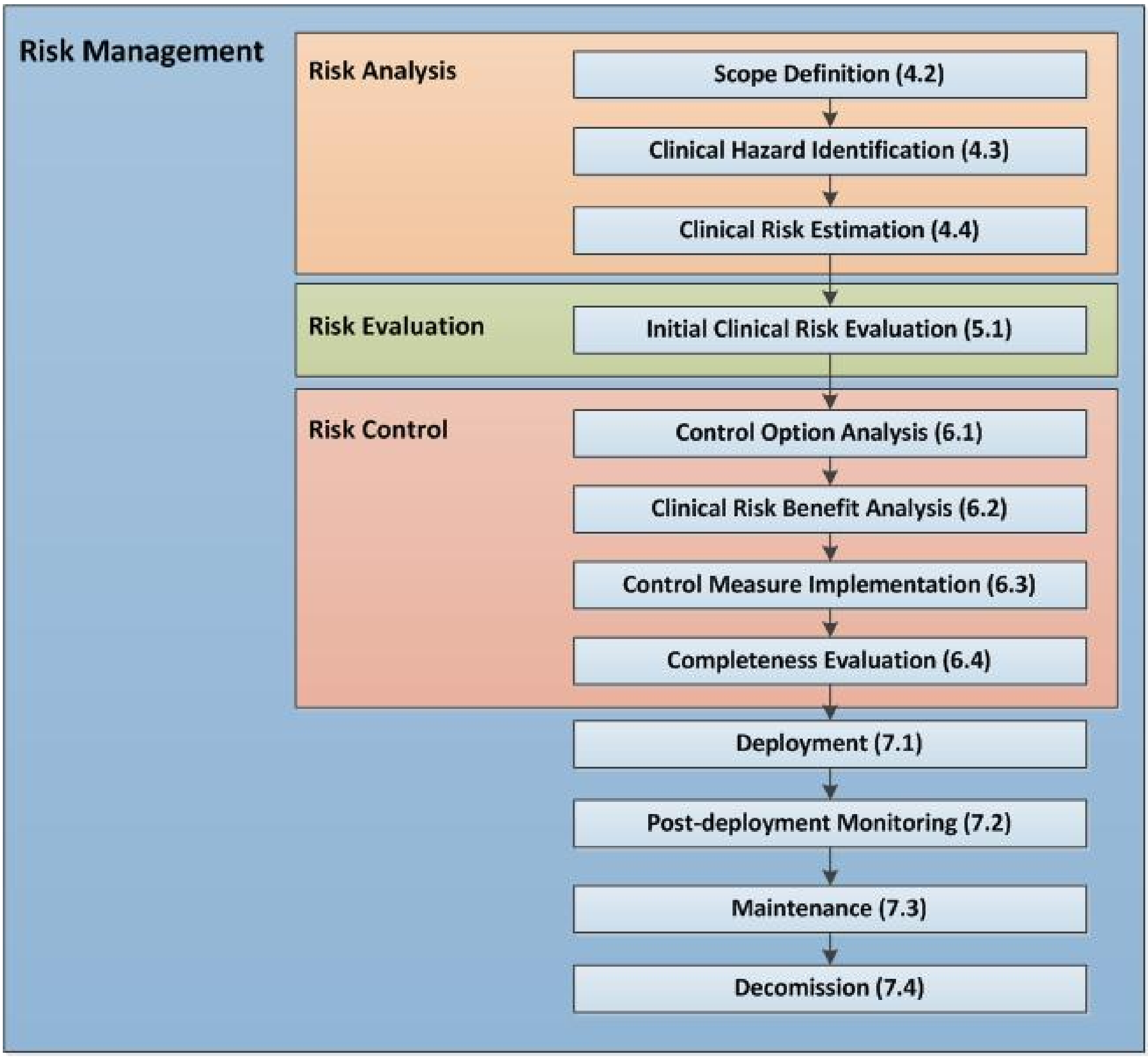
Risk Management
Risk Analysis
Scope Definition (4.2)
Clinical Hazard Identification (4.3)
Clinical Risk Estimation (4.4)
Risk Evaluation
Initial Clinical Risk Evaluation (5.1)
Risk Control
Control Option Analysis (6.1)
Clinical Risk Benefit Analysis (6.2)
Control Measure Implementation (6.3)
Completeness Evaluation (6.4)
Deployment (7.1)
Post-deployment Monitoring (7.2)
Maintenance (7.3)
Decomission (7.4)

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.*

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.

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.

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.

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